JINSHI DAISHU JICHU WENTI TANXI

近世代数基础

问题探析

齐晓梅　乔凤珠　编著



教育科学出版社

近世代数基础问题探析

JINSHI DAISHU JICHU WENTI TANXI

责任编辑／杨晓琳
封面设计／顾　童





ISBN 7-5041-3184-9
定价：39.00元

近世代数基础问题探析

齐晓梅　乔凤珠　编著

教育科学出版社
·北　京·

责任编辑　杨晓琳
版式设计　尹明好
责任校对　贾静芳
责任印制　曲凤玲

图书在版编目(CIP)数据

近世代数基础问题探析 / 齐晓梅，乔凤珠编著. —北京：教育科学出版社，2006.9
ISBN 7-5041-3184-9

Ⅰ. 近… Ⅱ. ①齐…②乔… Ⅲ. 抽象代数—基础理论—理论研究 Ⅳ. O153

中国版本图书馆 CIP 数据核字(2005)第 085318 号

出版发行	教育科学出版社	市场部电话	010—64989009
社　　址	北京·朝阳区安慧北里安园甲 9 号	编辑部电话	010—64989593
邮　　编	100101	网　　址	http://www.esph.com.cn
传　　真	010—64891796		
经　　销	各地新华书店		
印　　刷	保定市中画美凯印刷有限公司		
开　　本	787 毫米×1092 毫米　1/16		
印　　张	25.75	版　　次	2006 年 9 月第 1 版
字　　数	620 千	印　　次	2006 年 9 月第 1 次印刷
定　　价	39.00 元	印　　数	00 001—2 000 册

如有印装质量问题，请到所购图书销售部门联系调换。

前　　言

近世代数是现代数学的基础，也是现代科学的基础．它研究代数系统的代数结构，而代数结构是数学各种研究对象的一个重要的侧面．它介绍了现代代数学的基础知识和基本方法．数学的各个分支都或多或少地用到它的概念、理论和方法，即使应用很广的数值计算和计算机软件也要用到它，而且在理论物理和物理化学的部分分支中也有应用．它还是自然科学、工程科学、管理科学相关专业的重要基础之一．近世代数是高级科技人才进行深造的一个不可缺少的台阶．

近世代数在培养抽象思维能力和逻辑推理能力方面起着特殊的重要作用，不愧被称为抽象概念的宝塔、逻辑推理的楷模．正是由于其中概念的抽象性，推理的严谨性，方法的技巧性，从而给教者与学者带来了相当的困难．因此，依据近世代数基本内容，为了理论的系统与严谨，又不增加本书的篇幅，我们以张禾瑞著《近世代数基础》(1978 年修订本)一书为主，围绕近世代数的一些基本概念和基本定理，针对学习者学习过程中容易出现的问题，有的放矢地精心探索与分析，编写了本书．

本书内容包括：基本概念，群、环与域，整环里的因子分解和扩域．共十七章．每章都有以下四个部分．

一、基本问题问答．对基本概念和基本理论中的疑点和难点进行了详尽的阐述．

二、典型问题分析．根据近世代数基础中的一些代表性问题，进行了详细的剖析与注解．

三、讲与练．这部分包括围绕基础知识的问题的练习与比较重要的一些结论的讲解．

四、思考问题．这部分提供了一些紧密联系基本内容的问题，请读者独立思考．书后解答作为思考后的参考．

本书主要特点如下．

1. 释疑．注重分析基本概念和理论的内在联系与本质区分，释疑解惑．同时注意对基础知识的内涵与外延做出必要的、适当的分析．这样，便于读者对于基本内容能够融会贯通、深刻理解、扎实掌握和灵活应用．

2. 严谨．概念准确，分析论证严密详尽，有根有据．这一特点有助于培养读者深刻思考和缜密推理的能力．

3. 新颖．配有相当数量的命题的多种分析与论证，从各种不同的渠道，给出问题的解决方案．同时针对容易混淆的问题，给出了正、反例子和判断方法．这样，有利于读者开拓思维，发挥独立性和创造性，主动积极地进行思考．

本书适用于大专院校数学专业的相关教师与学生，以及有关的科学技术人员，而且十分有助于电大师生、函授生与自学成才者．

本书为海南大学学术著作出版基金资助出版，我们深表感谢．

对于错误和不妥之处，恭请读者指正．

编　者

符　　号

符号	含义
$a\in A$	元 a 属于集 A
$a\overline{\in}A$	元 a 不属于集 A
$B\subset A$	集 B 是集 A 的子集（或 A 包含 B）
$B\not\subset A$	集 B 不是集 A 的子集（或 A 不包含 B）
$A\cup B$	集 A 与集 B 的并
$A\cap B$	集 A 与集 B 的交
$\varnothing$	空集
ϕ	法则
$\forall$	对于任意的
$\exists$	存在
$\overline{\exists}$	不存在
$\exists\vert$	存在唯一
$\mathbb{N}$	自然数集
$\mathbb{Z}$	整数集
$\mathbb{Q}$	有理数集
$\mathbb{R}$	实数集
$\mathbb{C}$	复数集
$\mathbb{Z}^+$	正整数集
$\mathbb{Q}^+$	正有理数集
$\mathbb{R}^+$	正实数集
$P(A)$	集 A 的一切子集的集（A 的幂集）
$M_n(R)$	环 R 上的一切 n 阶方阵的集
$GL_n(F)$	数域 F 上的一切 n 阶可逆方阵的集
$\sim$	同态
$\not\sim$	不同态
$\cong$	同构
$\not\cong$	不同构
$a\equiv b(n)$	a 同余 b 模 n（或 a,b 对模 n 同余）
$\max\{a,b\}$	a 与 b 中的较大者

符号	含义
$\min\{a,b\}$	a 与 b 中的较小者
$\sum$	和
$\prod$	积
$\vert G\vert$	群 G 的阶
$\vert a\vert$	元 a 的阶
$(i_1\ i_2\cdots i_k)$	k-循环置换
S_n	n 次对称群
A_n	n 次交错群（或 n 次交代群）
$\mathbb{Z}_n$	整数模 n 的剩余类加群
(a)	由 a 生成的循环群或由 a 生成的主理想
(a,b)	由 a,b 生成的理想或 a,b 的最大公因数
$H<G$	H 是群 G 的子群
Ha,aH	子群 H 的右陪集，左陪集
$N\lhd G$	N 是群 G 的不变子群
$\ker\phi$	同态映射 ϕ 的核
G/N	群 G 对于不变子群 N 的商群
$\mathrm{ch}R$	环 R 的特征
$R[x]$	环 R 上的未定元 x 的多项式环
$R[x_1,x_2,\cdots,x_n]$	环 R 上无关未定元 $x_1,x_2,\cdots,x_n$ 的多项式环
$\deg f(x)$	多项式 $f(x)$ 的次数
$a\vert b$	a 整除 b（或 b 能被 a 整除）
$a\nmid b$	a 不整除 b（或 b 不能被 a 整除）
$[x]$	不大于实数 x 的最大整数
$F(S)$	添加集合 S 于域 F 所得的扩域
$F(a_1,a_2,\cdots,a_n)$	添加元素 $a_1,a_2,\cdots,a_n$ 于域 F 所得的扩域
$F(\alpha)$	单扩域
$(E:F)$	扩域 E 在域 F 上的次数

目　　录

第一章　集合、映射、代数运算

一、基本问题问答

1. B 不是 A 的子集的定义是什么？

答　$B \not\subset A \Leftrightarrow \exists a \in B$，使得 $a \overline{\in} A$.

2. B 不是 A 的真子集的定义是什么？

答　B 不是 A 的真子集

$\Leftrightarrow B \not\subset A$

或 $B \subset A$ 而 $\forall a \in A$ 有 $a \in B$

$\Leftrightarrow B \not\subset A$

或 $B = A$.

3. 空集$\varnothing$是任一集 A 的真子集吗？

答　不是．因为$\varnothing$不是$\varnothing$的真子集．应说$\varnothing$是任一非空集 A 的真子集.

4. 我们已经知道

$A_1 \times A_2 \times \cdots \times A_n = \left\{ (a_1, a_2, \cdots, a_n) \middle| a_i \in A_i \right\}$是 $A_1, A_2, \cdots, A_n$ 的卡氏积.

1)　若某 $A_i = \varnothing$，则 $A_1 \times A_2 \times \cdots \times A_n = ?$

2)　若 A_i 含 s_i 个元，$i = 1, 2, \cdots, n$，则 $A_1 \times A_2 \times \cdots \times A_n$ 含多少个元？

答　1)　某 $A_i = \varnothing$时，$A_1 \times A_2 \times \cdots \times A_n = \varnothing$.

2)　A_i 含 s_i 个元时，$A_1 \times A_2 \times \cdots \times A_n$ 含 $s_1 \times s_2 \times \cdots \times s_n$ 个元.

5. $A_1 \times A_2 \times \cdots \times A_n$ 到 D 的映射的定义是什么？

答　ϕ是 $A_1 \times A_2 \times \cdots \times A_n$ 到 D 的一个映射

$\Leftrightarrow$ 1)　$\forall (a_1, a_2, \cdots, a_n) \in A_1 \times A_2 \times \cdots \times A_n$，$\exists d \in D$，使得

$\phi(a_1, a_2, \cdots, a_n) = d$；

2)　$\forall (a_1, a_2, \cdots, a_n), (b_1, b_2, \cdots, b_n) \in A_1 \times A_2 \times \cdots \times A_n$，

若$(a_1, a_2, \cdots, a_n) = (b_1, b_2, \cdots, b_n)$，

则$\phi(a_1, a_2, \cdots, a_n) = \phi(b_1, b_2, \cdots, b_n)$.

注　这里要突出强调$\forall (a_1, a_2, \cdots, a_n) \in A_1 \times A_2 \times \cdots \times A_n$，象 d 的存在性、唯一性以及 $d \in D$，尤其要注意唯一性的验证方法.

6. $\circ$ 是 A 的代数运算的定义是什么？

答　$\circ$ 是 A 的代数运算

$\Leftrightarrow \circ$是一个 $A \times A$ 到 A 的映射

$\Leftrightarrow \circ$是一个 $A \times A$ 到 A 的代数运算．

注 $\circ$是 A 的代数运算

$\Leftrightarrow A$ 对于$\circ$封闭

$\Leftrightarrow\circ$是 A 的二元运算.

二、典型问题分析

1. $A=\{1,2,3,\cdots,100\}$. 找一个 $A\times A$ 到 A 的映射.

解 $\forall a,b\in A$,

$(a,b)\to a$;

$(a,b)\to b$;

$(a,b)\to 1$;

$(a,b)\to \max\{a,b\}$;

$\begin{cases}(a,b)\to a+1, & a\neq 100 \text{ 时},\\(a,b)\to 1, & a=100 \text{ 时};\end{cases}$

$\begin{cases}(a,b)\to b-1, & b\neq 1 \text{ 时},\\(a,b)\to 1, & b=1 \text{ 时};\end{cases}$

$(a,b)\to (-1)^{a+b}+2$;

$(a,b)\to |a-b|+1$;

$(a,b)\to \max\{a,b\}-\min\{a,b\}+1$;

	1	2	3	⋯	99	100
1	1	2	3	⋯	99	100
2	2	3	4	⋯	100	1
3	3	4	5	⋯	1	2
⋮	⋯	⋯	⋯	⋯	⋯	⋯
100	100	1	2	⋯	98	100

都是 $A\times A$ 到 A 的映射.

注 1) 读者应尽量多找出一些映射.

2) 下面命题"$A\times A$ 到 A 的映射是$(a,b)\to a$."不对,应说:

$$(a,b)\to a$$

是 $A\times A$ 到 A 的映射,因为 $A\times A$ 到 A 的映射不仅仅有

$$(a,b)\to a.$$

2. $A=\{$所有不等于零的偶数$\}$. 找一个集合 D,使得普通除法是 $A\times A$ 到 D 的代数运算.是不是找得到一个以上的这样的 D?

解 因为一个不等于零的偶数除以一个不等于零的偶数,所得的商永远是一个不等于零的有理数,所以 D 可取$\{$所有不等于零的有理数$\}$.

包含集$\{$所有不等于零的有理数$\}$的一切数集都可作为这样的 D.

3. $A=\{$所有不等于零的实数$\}$. $\circ$是普通除法：$a\circ b=\dfrac{a}{b}$. 这个代数运算适合不适合结合律？

解一 $\forall a,b,c\in A$,

$$(a\circ b)\circ c=\frac{a}{bc},\quad a\circ(b\circ c)=\frac{ac}{b}.$$

当 $c\neq\pm1$ 时，

$$(a\circ b)\circ c\neq a\circ(b\circ c),$$

从而$\circ$不适合结合律.

解二 取 $1,2,3\in A$,

$$(1\circ2)\circ3=\frac{1}{6},\quad 1\circ(2\circ3)=\frac{3}{2},$$

从而

$$(1\circ2)\circ3\neq1\circ(2\circ3).$$

所以$\circ$不适合结合律.

注 1) 在指出$(a\circ b)\circ c\neq a\circ(b\circ c)$时，必须明确是在 $c\neq\pm1$ 的条件下.

2) 不能说"A 不适合结合律"，因为运算律的主语是代数运算而不是集合．要说"$\circ$不适合结合律".

3) 在肯定$\circ$适合结合律时要按定义做出一般证明；否定时，举出一个反例即可.

4) 下面的说法是错误的："当 $c=\pm1$ 时，$(a\circ b)\circ c=a\circ(b\circ c)$，此时$\circ$适合结合律；当 $c\neq\pm1$时，$(a\circ b)\circ c\neq a\circ(b\circ c)$，此时$\circ$不适合结合律．因此$\circ$不一定适合结合律．"$\circ$只有适合结合律与不适合这两种情况．适合时，要求$\forall a,b,c\in A$，都有$(a\circ b)\circ c=a\circ(b\circ c)$；不适合时，只要有某一特殊情况，如 $c=2$ 时，$(a\circ b)\circ2\neq a\circ(b\circ2)$.

4. $A=\{a,b,c\}$. 由表

	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

所给的代数运算适合不适合结合律？

解 所给代数运算$\circ$适合结合律，即$\forall x,y,z\in A$，都有

$$(x\circ y)\circ z=x\circ(y\circ z).$$

为了证明这个结论，需要验证 $3\times3\times3=27$ 个(即三个不同元素允许重复的三元排列的个数)等式．我们要尽量简化计算，仔细观察一下这个代数运算有什么特点，我们发现表中第一行、第一列分别与表头的行、列相同，即$\forall x\in A$,

$$a\circ x=x,\quad x\circ a=x.$$

也就是说 a 左乘、右乘任何元不变，从而$\forall x,y\in A$,

$$(a\circ x)\circ y=x\circ y=a\circ(x\circ y);$$
$$(x\circ a)\circ y=x\circ y=x\circ(a\circ y);$$
$$(x\circ y)\circ a=x\circ y=x\circ(y\circ a).$$

这样，三个元中只要出现 a，我们就已验证完了．下面我们只需验证三个元中不出现 a 的情况，从而只剩下 $2\times2\times2=8$ 个（即两个相异元素允许重复的三元排列的个数）等式了．验证如下．

$$(b\circ b)\circ b=a=b\circ(b\circ b);$$
$$(b\circ b)\circ c=b=b\circ(b\circ c);$$
$$(b\circ c)\circ b=b=b\circ(c\circ b);$$
$$(b\circ c)\circ c=c=b\circ(c\circ c);$$
$$(c\circ b)\circ b=b=c\circ(b\circ b);$$
$$(c\circ b)\circ c=c=c\circ(b\circ c);$$
$$(c\circ c)\circ b=c=c\circ(c\circ b);$$
$$(c\circ c)\circ c=a=c\circ(c\circ c).$$

从而$\circ$适合结合律.

注 1) 验证结合律是一项基本训练．验证时，要对集中任意三个元素的一切可能的结合，一一加以检验，不要遗漏．对于有限集合，更要特别注意．当然应该尽量找出规律，几种情况可以集中一次验证.

2) 本题中的 a,b,c 是 A 中的确定的元，而不是任意元．因此取 A 中任意三个元时，不能用 a,b,c 表之，而要用其他符号，如 x,y,z 表之．不能由 $(a\circ b)\circ c=a\circ(b\circ c)$ 就得出$\circ$适合结合律的结论．

三、讲与练

1. 下列所述是否能组成集合？

1) 和他相貌相像的人.

2) 某城市里较大的商店.

3) 一些多项式.

4) 平面几何中的所有难题.

5) 分子是偶数的一切分数.

解 1)～5)都不能组成集合．因为所述事物是不清晰、不确定、含糊的.

2. 判断下列各命题是否正确.

1) 一架飞机是飞机场集合的一个元素.

2) $\{(0,1)\}$是方程 $x+y=1$ 的解的集合.

3) $\left\{x\,\middle|\,x-2=0\right\}=2$.

4) 当 A 是空集时，A 的子集组成的集合也是空集.

5) $\varnothing\subset\varnothing$.

6) $\varnothing\in\left\{\{\varnothing\}\right\}$.

7)　$\{\varnothing\}\not\subset\Big\{\{\varnothing\}\Big\}$.

8)　$\{\varnothing\}\in\Big\{\{\varnothing\}\Big\}$.

9)　$\Big\{n\,\Big|\,2<n<3, n\in\mathbb{N}\Big\}=\varnothing$.

10)　$2\in\Big\{\{2\}\Big\}$.

11)　$\{3\}\subset\Big\{\{3\}\Big\}$.

12)　若 $x\in B, B\in C$，则 $x\in C$.

解　1)～4)都错，5)～9)都对，10)～12)都错.

3. 证明：若集 A 含有 n 个不同元素，则 A 共有 2^n 个不同的子集.

证一　空集是 A 的子集，有 $1=\mathrm{C}_n^0$ 个．由一个元素组成的子集有 C_n^1 个；由两个元素组成的子集有 C_n^2 个；由 i 个元素组成的子集有 C_n^i 个，$i=1,2,\cdots,n$. 因此 A 的所有子集的个数是

$$\mathrm{C}_n^0+\mathrm{C}_n^1+\mathrm{C}_n^2+\cdots+\mathrm{C}_n^n=(1+1)^n=2^n.$$

证二　对 A 的元的个数作数学归纳法.

1)　$n=0$ 时，即 $A=\varnothing$，A 共有 $2^0=1$ 个子集.

2)　假设 $n=k$ 时，命题成立．今看 $n=k+1$ 时.

设 A_1 恰有 $k+1$ 个元，取 $a\in A_1$，但 $a\,\overline{\in}\,A$ 且 $A_1=A\cup\{a\}$. 对于 A 的每一子集 H 都有 A_1 的两个子集 H 或 $H\cup\{a\}$，由这一过程可以获得 A_1 的所有子集．因此 A_1 的子集的个数恰为 A 的子集的个数的 2 倍．由归纳假设，A 的子集的个数为 2^k，从而 A_1 的子集的个数为 $2\cdot 2^k=2^{k+1}$.

由归纳原理，命题得证.

证三　当 $n=0$ 时，命题显然成立。当 $n\neq 0$ 时，设 $A=\{a_1,a_2,\cdots,a_n\}$，即 $a_i\in$子集或 $a_i\,\overline{\in}$子集($i=1,2,\cdots,n$)，共有两种状态．因此 A 有 $\underbrace{2\times 2\times\cdots\times 2}_{n个}=2^n$ 个子集.

4. 若集 A 与 B 分别含有 n 与 m 个不同的元，问共有多少个不同的 A 到 B 的映射？

解　因为对于每一个 $a_i\in A, i=1,2,\cdots,n$，在 B 中取象的方法都有 m 个，所以 A 到 B 的全部映射的个数是

$$\underbrace{m\cdot m\cdot\cdots\cdot m}_{n个}=m^n.$$

5. 普通除法是不是复数集 $\mathbb{C}$ 的一个代数运算？

解　不是．因为 $1,0\in\mathbb{C}$，但 $\dfrac{1}{0}$ 无意义.

6. 设 $A=B=\mathbb{Z}$.

$\oplus$：普通加法是 A 的代数运算.

$\odot$：$b\odot a=b+1$ 是 $B\times A$ 到 A 的代数运算.

问 $\odot$，$\oplus$ 是否适合第一分配律？

解一　$\forall a_1,a_2\in A, b\in B$，

$$b\odot(a_1\oplus a_2)=b+1.$$

$$(b\odot a_1)\oplus(b\odot a_2)=(b+1)+(b+1)=2(b+1).$$

当 $b\neq -1$ 时，

$$b+1\neq 2(b+1).$$

所以$\odot$，$\oplus$不适合第一分配律.

解二 取 $2,3\in A,1\in B$，

$$1\odot(2\oplus 3)=1+1=2,$$

$$(1\odot 2)\oplus(1\odot 3)=(1+1)+(1+1)=4,$$

从而

$$1\odot(2\oplus 3)\neq(1\odot 2)\oplus(1\odot 3).$$

所以$\odot$，$\oplus$不适合第一分配律.

7. 若集 A 的代数运算$\odot$，$\oplus$适合第一分配律，则$\odot$，$\oplus$一定适合第二分配律吗？

解 未必．例，取 A 为正实数集$\mathbb{R}^+$.

$$\odot: a\odot b=\frac{b}{a},\quad \oplus: a\oplus b=a+b$$

是$\mathbb{R}^+$的两个代数运算．因

$$b\odot(a_1\oplus a_2)=b\odot(a_1+a_2)=\frac{a_1+a_2}{b}=\frac{a_1}{b}+\frac{a_2}{b}=(b\odot a_1)\oplus(b\odot a_2).$$

故$\odot$，$\oplus$适合第一分配律．取 $a_1=1,a_2=1,b=2$，

$$(a_1\oplus a_2)\odot b=(1+1)\odot 2=\frac{2}{2}=1,\quad (a_1\odot b)\oplus(a_2\odot b)=\frac{2}{1}+\frac{2}{1}=4,$$

从而$\odot$，$\oplus$不适合第二分配律．

四、思考问题

1. 下列所述是否能组成集合.

1） 和他是好朋友的人.

2） 好玩的玩具.

3） 平面上与某点靠近的点.

4） 很小的整数.

5） 某次数学考试所有高分数的人.

6） 老年人.

2. 判断下列各命题是否正确.

1） 一枝铅笔是铅笔盒集合的一个元素.

2） 赵杰是北京市中学集合的一个元素.

3） $\varnothing\in\varnothing$.

4） $\varnothing\subset\{\varnothing\}$.

5) $\varnothing\in\{\varnothing\}$.

6) $\varnothing\subset\left\{\{\varnothing\}\right\}$.

7) $\varnothing\in\left\{\varnothing,\{\varnothing\}\right\}$.

8) $\varnothing\subset\left\{\varnothing,\{\varnothing\}\right\}$.

9) $\{\varnothing\}\overline{\in}\varnothing$.

10) $\{\varnothing\}\subset\{\varnothing\}$.

11) $\{\varnothing\}\overline{\in}\{\varnothing\}$.

12) $\{\varnothing\}\in\left\{\varnothing,\{\varnothing\}\right\}$.

13) $\left\{\{\varnothing\}\right\}\subset\left\{\varnothing,\{\varnothing\}\right\}$.

14) $\left\{x\,\middle|\,x=x+1,x\in\mathbb{Z}\right\}=\varnothing$.

15) $\{3\}\subset\{3,1\}$.

16) 若 $A\in B$，$B\not\subset C$，则 $A\overline{\in}C$.

17) 若 $x\in A\cup B$，则 $a\in A$.

18) 若 $x\in A$，则 $a\in A\cap B$.

19) $\varnothing\in A$.

20) $(\varnothing\cap A)\subset A$.

21) $A\in(\varnothing\cup A)$.

22) $\{a,b\}\subset\left\{\{a,b\},c\right\}$.

23) $\{a,b\}\in\left\{a,b,c\right\}$.

24) $\varnothing\subset\left\{a,\varnothing\right\}$.

25) $\varnothing\in\left\{a,\varnothing\right\}$.

26) $\{a,b\}\cap\{b,c\}\subset\{a,b\}\cup\{b,c\}$.

27) 任何一个集合都存在真子集.

3. 从以下五个命题中选出正确的命题．$A\times B$

1) 总含有比 A 多的元素.

2) 与 $B\times A$ 的交总是空的.

3) 含有 A 与 B 的全部元素.

4) 有与 $B\times A$ 一样多的元素.

5) 与 $B\times A$ 相等.

4. 设 $A_n=(n,+\infty)=\left\{x\in\mathbf{R}\,\middle|\,n<x<+\infty\right\}$，$n=0,1,2,\cdots$，求 $\bigcup\limits_{i=0}^{+\infty}A_i$，$\bigcap\limits_{i=0}^{+\infty}A_i$.

5. 设 $A_n=\left\{x\in\mathbf{Q}\,\middle|\,|x|<\dfrac{1}{n}\right\}$，$n=1,2,\cdots$，求 $\bigcup\limits_{i=1}^{+\infty}A_i$，$\bigcap\limits_{i=1}^{+\infty}A_i$.

6. 求证：$A=B \Leftrightarrow A\cup B\subset A\cap B$.

7. 设 $A=\left\{x \middle| x^2-16<0\right\}$，$B=\left\{x \middle| x^2-4x+3\geqslant 0\right\}$，求 $A\cap B$.

8. 设 $f(x)$，$g(x)$是实多项式，其实根集合分别记为 A 和 B，求证：

1) 多项式 $f(x)g(x)$实根的集合为 $A\cup B$.

2) 多项式 $f^2(x)+g^2(x)$实根的集合为 $A\cap B$.

9. 设集 A 恰含 n 个元，试将 A 分成两个不相交的子集 A_1 与 A_2，使 $A_1\times A_2$ 含的元的个数最多.

10. 试判断下列各法则ϕ是否为 A 到 B 的映射.

1) $A=B=\mathbb{Z}$，$\phi: n\rightarrow n+1$.

2) $A=B=\mathbb{N}$，$\phi: x\rightarrow x^2-1$.

3) $A=\mathbb{N}$，$B=\left\{x\in\mathbb{Z} \middle| x>0\right\}$，$\phi: n\rightarrow |n|$.

4) $A=B=\mathbb{N}$，

$$\phi:\begin{cases} n\rightarrow 1, & \text{当 } 2\mid n \text{ 时；} \\ n\rightarrow 2, & \text{当 } 2\nmid n \text{ 时.}\end{cases}$$

5) $A=B=\mathbb{R}$，$\phi: a\rightarrow \dfrac{a+1}{a-1}$.

6) $A=\mathbb{Z}$，$B=\mathbb{Q}$，$\phi: x\rightarrow y=\dfrac{1}{x}$.

7) $A=B=\mathbb{R}$，$\phi: a\rightarrow\sqrt{a+1}$.

8) $A=B=\mathbb{R}$，$\phi: x\rightarrow\sqrt{x}$.

9) $A=\{4,6,8\}$，$B=\{1,2,3\}$，

$\phi: a\rightarrow b$，b 是 a 的约数.

10) $A=B=\mathbb{R}$，$\phi: a\rightarrow \lg(a+1)$.

11) $A=$数域 F 上一元多项式集合 $F[x]$，

$B=$非负整数集$\{0,1,2,\cdots\}$，

$\phi: f(x)\rightarrow \deg f(x)$.

12) $A=$数域 F 上的 n 阶方阵的集合 $M_n(F)$，

$B=\{0,1,2,\cdots,n\}$，

$\phi: (a_{ij})\rightarrow$秩$(a_{ij})$.

11. 问下列ϕ_1 与ϕ_2 有何关系？

1) $A=\{0,2\}$，$B=\{0,4\}$，

$\phi_1: x\rightarrow x^2$，$\phi_2: x\rightarrow 2x$.

2) $A=\mathbb{R}$，$B=\left\{x\in\mathbb{R} \middle| x\geqslant 0\right\}$，

$\phi_1: a\rightarrow |a|$，$\phi_2: a\rightarrow\sqrt{a^2}$.

12. 下列各法则$\circ$是不是集 A 的代数运算？

1) $A=\{a,b\}$，

$\circ: (a,b)\rightarrow a\circ b=a$，

$(b,a)\to b\circ a=b.$

2) $A=\mathbb{Q}$,

$\circ:(a,b)\to a\circ b=a$,当 $a>0$ 时;

$(a,b)\to a\circ b=b$,当 $a<0$ 时.

3) $A=$数域 F 上的一元多项式集合 $F[x]$,

$\circ:(f(x),g(x))\to f(x)\circ g(x)=d(x)$,其中 $d(x)$是 $f(x),g(x)$的最大公因式.

4) $A=\mathbb{Z}$,

$\circ:(a,b)\to a\circ b=a^b.$

5) $A=\mathbb{Q}$,

$\circ:(a,b)\to a\circ b=10^{a+b}.$

6) $A=\mathbb{Q}$,

$\circ:(a,b)\to a\circ b=b\sqrt{a}+2b^2.$

7) $A=$正有理数集$\mathbb{Q}^+$,

$\circ:(a,b)\to a\circ b=\sqrt{ab}.$

8) $A=\mathbb{Q}$,

$\circ:(\frac{b}{a},\frac{d}{c})\to\frac{b}{a}\circ\frac{d}{c}=\frac{b+d}{ac}.$

9) $A=$集 B 的一切子集的集 $P(B)$,

$\circ:(H,K)\to H\circ K=H\cap K.$

10) $A=P(B)$,

$\circ:(H,K)\to H\circ K=H\cup K.$

11) $A=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\-1&0\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\begin{pmatrix}0&-1\\1&0\end{pmatrix}\right\}$,$\circ$是普通矩阵乘法.

12) $A=$数域 F 上 n 维向量空间,$e_1,e_2,\cdots,e_n$ 是 A 的一个基,$\forall(a,b)\in A\times A$,

$$a=\alpha_1e_1+\alpha_2e_2+\cdots+\alpha_ne_n,$$
$$b=\beta_1e_1+\beta_2e_2+\cdots+\beta_ne_n.$$
$$\circ:(a,b)\to a\circ b=\alpha_1\beta_1+\alpha_2\beta_2+\cdots+\alpha_n\beta_n.$$

13. 设集 A 恰含 n 个元,问 A 中最多有多少种代数运算?

14. 设 $A=\{a,b,c,d\}$,$\circ$是 A 的代数运算.问在不交换元素次序的情况下,a,b,c,d 共有多少种不同的加括号步骤?

15. 以下各代数运算$\circ$是否适合结合律和交换律?

1) $\mathbb{Z}$的代数运算:$a\circ b=a^2+b^2$.

2) $\mathbb{N}$的代数运算:$a\circ b=a^b$.

3) $\mathbb{Q}$的代数运算:$a\circ b=b$.

4) $\mathbb{R}$的代数运算:$a\circ b=ab^2$.

16. 设 $A=\{a,b,c,d\}$,其运算表如下:

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

证明：$\circ$适合结合律.

17. 设集 A 对于$\circ$封闭，且$\circ$适合结合律，$\forall a,b\in A$，若 $a\neq b$，有 $a\circ b\neq b\circ a$. 证明：

1) $\forall a\in A$，有 $a\circ a=a$.

2) $\forall a,b\in A$，有 $a\circ b\circ a=a$.

3) $\forall a,b,c\in A$，有 $a\circ b\circ c=a\circ c$.

18. 设集 A 对于$\circ$封闭，且$\circ$适合结合律，交换律，若 $a\circ a=a$，$b\circ b=b$，证明：

$$(a\circ b)\circ(a\circ b)=a\circ b.$$

19. 修改以下各命题中错误的表示方法.

1) 从 A 中任意取出三个元素可表为

$$\forall a、b、c\in A.$$

2) 卡氏积 $A_1\times A_2$ 的元素可表为$(a_1\ a_2)$，$a_i\in A_i$，$i=12$.

3) A 中含 n 个元素 $a_1\ a_2\cdots a_n$，即

$$A=\{a_i\,|\,i=1,2\cdots\}.$$

4) a,b 都不等于零，即 $a\neq b\neq 0$.

第二章　一一映射、同态、同构

一、基本问题问答

1. A 到 $\bar{A}$ 的满射的定义是什么？

答　ϕ是 A 到 $\bar{A}$ 的一个满射

$\Leftrightarrow$ 1)　ϕ是 A 到 $\bar{A}$ 的一个映射；

2)　$\forall \bar{a}\in\bar{A}$，$\exists a\in A$，使得$\phi(a)=\bar{a}$

（即 $\bar{A}$ 的每一个元在ϕ下都在 A 中有逆象）.

2. A 到 $\bar{A}$ 的单射的定义是什么？

答　ϕ是 A 到 $\bar{A}$ 的一个单射

$\Leftrightarrow$ 1)　ϕ是 A 到 $\bar{A}$ 的一个映射；

2)　$\forall a,b\in A$，若$\phi(a)=\phi(b)$，则 $a=b$

（即 $\bar{A}$ 的每一个元在ϕ下若有逆象，则逆象唯一）.

注　映射要求象唯一，而单射还要求逆象唯一.

二、典型问题分析

1. $A=$｛所有大于零的实数｝，$\bar{A}=$｛所有实数｝. 找一个 A 与 $\bar{A}$ 间的一一映射.

解　$\forall a\in A$，

$$a\to \ln a;$$

$$a\to \log_x a,$$

其中 x 是一个固定的不等于 1 的正实数；

$$a\to a-\frac{1}{a};$$

$$\begin{cases} a\to \dfrac{1}{a}, & 0<a\leqslant 1 \text{ 时},\\ a\to 2-a, & a>1 \text{ 时}\end{cases}$$

都是 A 与 $\bar{A}$ 间的一一映射.

注　为了训练分析能力，可进一步思考以下问题：$A=$｛所有大于零的实数｝，$\bar{A}=$｛所有实数｝.

1)　找一个 $\bar{A}$ 与 A 间的一一映射，也就是找一个 A 与 $\bar{A}$ 间的一一映射的逆映射.

2)　找一个 $\bar{A}$ 到 A 的单射，但不是满射.

3)　找一个 $\bar{A}$ 到 A 的满射，但不是单射.

4) 找一个$\overline{A}$到A的映射,但不是单射也不是满射.

5) 设普通乘法是A的代数运算,普通加法是$\overline{A}$的代数运算.找一个A与$\overline{A}$间对于乘法和加法来说的同构映射.

事实上,1) $\forall \bar{a}\in\overline{A}$,

$$\bar{a}\to e^{\bar{a}},$$

其中

$$e=2.718\cdots;$$

$$\bar{a}\to x^{\bar{a}};$$

其中x是一个固定的不等于1的正实数;

$$\bar{a}\to\frac{\bar{a}+\sqrt{\bar{a}^{2}+4}}{2};$$

$$\begin{cases}\bar{a}\to\dfrac{1}{\bar{a}}, & \bar{a}\geqslant 1\text{ 时},\\ \bar{a}\to 2-\bar{a}, & \bar{a}<1\text{ 时}\end{cases}$$

都是$\overline{A}$与A间的一一映射.

2) $\forall \bar{a}\in\overline{A}$,

$$\phi:\bar{a}\to e^{\bar{a}}+1$$

是$\overline{A}$到A的单射.但ϕ不是满射.因为取$1\in A$,假定$\exists\,\bar{a}\in\overline{A}$,使得$\phi(\bar{a})=1$,即$e^{\bar{a}}+1=1$,从而$e^{\bar{a}}=0$,此为不可能.故1在$\phi$下无逆象.所以$\phi$不是满射.

3) $\forall \bar{a}\in\overline{A}$,

$$\phi:\bar{a}\to\bar{a}^{2},\quad \bar{a}\neq 0\text{ 时},$$
$$\bar{a}\to 1,\quad \bar{a}=0\text{ 时}$$

是$\overline{A}$到A的满射但不是单射.

4) $\forall \bar{a}\in\overline{A}$,

$$\phi:\bar{a}\to 1$$

是$\overline{A}$到A的映射,但不是单射也不是满射.

5) $\forall a\in A$,

$$\phi:a\to\log_x a$$

(其中x是一个固定的不等于1的正实数)是A与$\overline{A}$间对于乘法和加法来说的同构映射.

A与$\overline{A}$的代数性质完全一样.例如,在A中,等比数列前n项的积$p_n=a_1a_2\cdots a_n$可用下列公式来表示:

$$p_n=\sqrt{(a_1a_n)^n}.$$

令

$$\phi:a_1\to\bar{a}_1=\log_x a_1,$$
$$a_2\to\bar{a}_2=\log_x a_2,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$a_n\to\bar{a}_n=\log_x a_n.$$

则在$\overline{A}$中,$\bar{a}_1,\bar{a}_2,\cdots,\bar{a}_n$是等差数列前$n$项,其和$\bar{p}_n=\bar{a}_1+\bar{a}_2+\cdots+\bar{a}_n$就可用下列公式来表示:

$$\bar{p}_n=\frac{n(\bar{a}_1+\bar{a}_n)}{2}.$$

2. $A=\{$所有大于或等于零的实数$\}$，$\bar{A}=\{$所有实数 $\bar{a}$，$0\leqslant\bar{a}\leqslant1\}$．找一个 A 到 $\bar{A}$ 的满射.

解　$\forall a\in A$，

$$a\to|\sin a|;$$

$$a\to|\cos a|;$$

$$a\to\sin^{2n}a\text{，}n\text{ 是一个固定正整数；}$$

$$a\to\cos^{2n}a\text{，}n\text{ 是一个固定正整数；}$$

$$a\to\left(\frac{1}{2}\right)^a;$$

$$a\to\frac{|a-1|}{a+1};$$

$$\begin{cases}a\to0, & 0\leqslant a<1\text{ 时，}\\ a\to\dfrac{1}{a}, & a\geqslant1\text{ 时；}\end{cases}$$

$$\begin{cases}a\to a, & 0\leqslant a\leqslant1\text{ 时，}\\ a\to\dfrac{1}{a}, & a>1\text{ 时；}\end{cases}$$

$$\begin{cases}a\to a, & 0\leqslant a\leqslant1\text{ 时，}\\ a\to1, & a>1\text{ 时；}\end{cases}$$

$$\begin{cases}a\to a, & 0\leqslant a\leqslant1\text{ 时，}\\ a\to0, & a>1\text{ 时；}\end{cases}$$

$$\begin{cases}1\to1,\\ a\to\dfrac{a}{a+1}, & a\neq1\text{ 时}\end{cases}$$

都是 A 到 $\bar{A}$ 的满射.

3. 假定ϕ是 A 与 $\bar{A}$ 间的一个一一映射，a 是 A 的一个元. 求$\phi^{-1}[\phi(a)]$，$\phi[\phi^{-1}(a)]$

解　设$\phi^{-1}[\phi(a)]=x$，则$\phi(x)=\phi(a)$. 因ϕ是单射，故 $x=a$，从而

$$\phi^{-1}[\phi(a)]=a.$$

当 $a\overline{\in}\bar{A}$ 时，$\phi[\phi^{-1}(a)]$无意义.

当 $a\in\bar{A}$ 时，设$\phi[\phi^{-1}(a)]=y$，则$\phi^{-1}(a)=\phi^{-1}(y)$. 因$\phi^{-1}$是单射，故 $y=a$，从而

$$\phi[\phi^{-1}(a)]=a.$$

4. $A=\{$所有实数 $x\}$. A 的代数运算是普通乘法．以下映射是不是 A 到 A 的一个子集 $\bar{A}$ 的同态满射？

$$x\to x^2.$$

解　取 $\bar{A}=\{$所有大于或等于零的实数$\}$，则 $\bar{A}\subset A$，且普通乘法也是 $\bar{A}$ 的一个代数运算.

$$x\to x^2$$

是 A 到 $\bar{A}$ 的一个同态满射．事实上，

1) $\forall x\in A, x^2$ 是一个唯一确定的大于或等于零的实数，所以 $x\rightarrow x^2$ 是 A 到 $\overline{A}$ 的一个映射.

2) $\forall \overline{x}\in\overline{A}$，有 $\overline{x}\geqslant 0$. 假定 $\exists x\in A$，使得 $x^2=\overline{x}$，那么 $x=\pm\sqrt{\overline{x}}$. 因此 $\exists\sqrt{\overline{x}}\in A$，使得

$$\sqrt{\overline{x}}\rightarrow(\sqrt{\overline{x}})^2=\overline{x}.$$

所以 $x\rightarrow x^2$ 是 A 到 $\overline{A}$ 的一个满射.

3) $\forall x,y\in A$，

$$x\rightarrow x^2,\quad y\rightarrow y^2,$$
$$xy\rightarrow(xy)^2=x^2y^2.$$

所以 $x\rightarrow x^2$ 是 A 到 $\overline{A}$ 的一个同态满射.

注 1) 在证明满射时，要特别注意按照满射的定义，首先从第二个集合 $\overline{A}$ 中任意取出一个元 $\overline{x}$，再去寻求 $\overline{x}$ 在这个映射下的逆象．而绝不能把 x 的象 $x^2\in\overline{A}$ 取来，就说因为 x^2 有逆象 x，从而该映射是满射.

2) 在肯定 $x\rightarrow x^2$ 是 A 到 $\overline{A}$ 的一个同态满射时，首先要明确指出 $\overline{A}$ 是 A 的什么样的具体的子集.

3) 这里 $\overline{A}$ 的代数运算与 A 的代数运算相同，都是普通乘法．一般情况，集 A 的代数运算未必是其子集的代数运算.

4) $\forall x,y\in A$，若 $x^2=y^2$，则 $x=\pm y$. 所以 $x\rightarrow x^2$ 不是 A 到 $\overline{A}$ 的单射.

5. 假定 A 和 $\overline{A}$ 对于代数运算 $\circ$ 和 $\bar{\circ}$ 来说同态，$\overline{A}$ 和 $\overline{\overline{A}}$ 对于代数运算 $\bar{\circ}$ 和 $\bar{\bar{\circ}}$ 来说同态．证明：A 和 $\overline{\overline{A}}$ 对于代数运算 $\circ$ 和 $\bar{\bar{\circ}}$ 来说同态.

证 因 $A\sim\overline{A}$，故由定义知存在一个 A 到 $\overline{A}$ 对于代数运算 $\circ$ 和 $\bar{\circ}$ 来说的同态满射 ϕ_1. 因 $\overline{A}\sim\overline{\overline{A}}$，故由定义知存在一个 $\overline{A}$ 到 $\overline{\overline{A}}$ 对于代数运算 $\bar{\circ}$ 和 $\bar{\bar{\circ}}$ 来说的同态满射 ϕ_2. 规定法则：$\forall a\in A$，

$$\phi: a\rightarrow\phi(a)=\phi_2(\phi_1(a)).$$

则 ϕ 是 A 到 $\overline{\overline{A}}$ 对于代数运算 $\circ$ 和 $\bar{\bar{\circ}}$ 来说的同态满射．事实上，

1) $\forall a\in A$，因 ϕ_1 是映射，故 $\exists|\,\phi_1(a)\in\overline{A}$. 对于 $\phi_1(a)\in\overline{A}$ 来说，因 ϕ_2 是映射，故 $\exists|\,\phi_2(\phi_1(a))\in\overline{\overline{A}}$，使得 $\phi(a)=\phi_2(\phi_1(a))$. 所以 ϕ 是 A 到 $\overline{\overline{A}}$ 的映射.

2) $\forall\overline{\overline{a}}\in\overline{\overline{A}}$，因 ϕ_2 是满射，故 $\exists\overline{a}\in\overline{A}$，使得 $\phi_2(\overline{a})=\overline{\overline{a}}$. 对于 $\overline{a}\in\overline{A}$ 来说，因 ϕ_1 是满射，故 $\exists a\in A$，使得 $\phi_1(a)=\overline{a}$，从而 $\exists a\in A$，使得

$$\phi(a)=\phi_2(\phi_1(a))=\phi_2(\overline{a})=\overline{\overline{a}}.$$

所以 ϕ 是 A 到 $\overline{\overline{A}}$ 的满射.

3) $\forall a,b\in A$，

$$\begin{aligned}\phi:\ & a\rightarrow\phi_2(\phi_1(a)),\\ & b\rightarrow\phi_2(\phi_1(b)),\\ & a\circ b\rightarrow\phi_2(\phi_1(a\circ b)).\end{aligned}$$

因 ϕ_1 是同态映射，故 $\phi_1(a\circ b)=\phi_1(a)\,\bar{\circ}\,\phi_1(b)$. 又因 ϕ_2 是同态映射，从而

$$\begin{aligned}\phi(a\circ b)&=\phi_2(\phi_1(a\circ b))\\ &=\phi_2(\phi_1(a)\,\bar{\circ}\,\phi_1(b))\end{aligned}$$

$$=\phi_2(\phi_1(a))\bar{\bar{\circ}}\phi_2(\phi_1(b))$$

$$=\phi(a)\bar{\bar{\circ}}\phi(b).$$

综上所述，知ϕ是 A 到 $\bar{\bar{A}}$ 对于代数运算$\circ$和$\bar{\bar{\circ}}$来说的同态满射，于是 $A\overset{\phi}{\sim}\bar{\bar{A}}$.

注 1) 对于此命题的证明，有的初学者叙述不好．注意首先给出ϕ_1 与ϕ_2，再规定ϕ，然后证明ϕ是 A 到 $\bar{\bar{A}}$ 的同态满射.

2) 此命题说明同态具有传递性.

3) ϕ_1 是 A 到 $\bar{A}$ 的映射，ϕ_2 是 $\bar{A}$ 到 $\bar{\bar{A}}$ 的映射，则

$$\phi: a\rightarrow\phi(a)=\phi_2(\phi_1(a))$$

是 A 到 $\bar{\bar{A}}$ 的映射．我们把ϕ叫做ϕ_1 与ϕ_2 的合成，记为$\phi=\phi_2\ \phi_1$.

4) 将此命题中的同态改为同构，命题仍成立.

6. $A=\{a,b,c\}$. 代数运算$\circ$由下表给定

	a	b	c
a	c	c	c
b	c	c	c
c	c	c	c

找出所有 A 的一一变换．对于代数运算$\circ$来说，这些一一变换是否都是 A 的自同构?

解 所有 A 的一一变换共有 $C_3^1\cdot C_2^1\cdot C_1^1=6$ 个，即

$$\tau_1: a\rightarrow a,\ b\rightarrow b,\ c\rightarrow c;$$

$$\tau_2: a\rightarrow a,\ b\rightarrow c,\ c\rightarrow b;$$

$$\tau_3: a\rightarrow b,\ b\rightarrow a,\ c\rightarrow c;$$

$$\tau_4: a\rightarrow b,\ b\rightarrow c,\ c\rightarrow a;$$

$$\tau_5: a\rightarrow c,\ b\rightarrow a,\ c\rightarrow b;$$

$$\tau_6: a\rightarrow c,\ b\rightarrow b,\ c\rightarrow a.$$

设 τ 是 A 的一个一一变换，则

$$\tau\text{是} A \text{的自同构}\Leftrightarrow\forall x,y\in A,\tau(x\circ y)=\tau(x)\circ\tau(y)$$

$$\Leftrightarrow\tau(c)=c.$$

由此得出：有且只有 τ_1,τ_3 是 A 的自同构.

注 要说明有且只有 τ_1,τ_3 是 A 的自同构的理由.

7. $A=\{$所有有理数$\}$. 找一个 A 的对于普通加法来说的自同构（映射 $x\leftrightarrow x$ 除外）.

解 $\forall x\in A$，令

$$\phi_k: x\rightarrow kx,$$

这里 k 是不等于零且不等于 1 的一个有理数，则ϕ_k 是一个 A 的对于普通加法来说的自同构．事实上，

1) $\forall x\in A$，$\exists|\,kx\in A$，使得

$$\phi_k: x\rightarrow kx.$$

2) $\forall y\in A$，若 $y=kx$，则因 $k\neq 0$，故 $x=\frac{y}{k}$，从而 $\exists \frac{y}{k}\in A$，使得

$$\phi_k:\frac{y}{k}\to k\left(\frac{y}{k}\right)=y.$$

3) $\forall x,y\in A$，若$\phi(x)=kx=ky=\phi(y)$，则因 $k\neq 0$，故 $x=y$.

4) $\forall x,y\in A$，

$$\phi_k:x\to kx,\ y\to ky.$$

则

$$\phi_k:x+y\to k(x+y)=kx+ky.$$

综上知，ϕ_k 是 A 的对于普通加法来说的一个自同构．因 $k\neq 1$，故ϕ_k 不是映射 $x\leftrightarrow x$.

注 1) 这里 k 是不等于零且不等于 1 的任意一个有理数，因此，A 的对于普通加法来说的自同构有无穷多个.

2) 还可以进一步证明：A 只有以下的对于加法来说的自同构：

$$\phi_k:x\to kx,$$

这里 k 是任意一个不等于零的有理数.

证明如下：设 τ 是 A 的任意一个对于普通加法来说的自同构．设

$$\tau:0\to\bar{0}.$$

我们先来看看 $\bar{0}$ 是 A 中的哪一个有理数．$\forall \bar{a}\in A$，因 τ 是 A 到 A 的满射，故 $\exists a\in A$，使得

$$\tau:a\to\bar{a}.$$

由 τ 保持运算，有

$$\tau:a+0\to\bar{a}+\bar{0}.$$

而 $a+0=a$，又 τ 是 A 到 A 的映射，从而 $\bar{a}+\bar{0}=\bar{a}$. 所以 $\bar{0}=0$. 由此知

$$\tau:0\to 0. \tag{1}$$

设

$$\tau:1\to k, \tag{2}$$

其中 k 是一个有理数．因 τ 是单射，故 $k\neq 0$.

对于$\frac{1}{n}\in A$，其中 n 是正整数．由 τ 保持运算，有

$$\tau:n\left(\frac{1}{n}\right)=\underbrace{\frac{1}{n}+\frac{1}{n}+\cdots+\frac{1}{n}}_{n个}\to\underbrace{\tau\left(\frac{1}{n}\right)+\tau\left(\frac{1}{n}\right)+\cdots+\tau\left(\frac{1}{n}\right)}_{n个}=n\tau\left(\frac{1}{n}\right).$$

又由(2)，有

$$\tau:n\left(\frac{1}{n}\right)=1\to k.$$

而 τ 是映射，从而 $n\tau\left(\frac{1}{n}\right)=k$. 所以 $\tau\left(\frac{1}{n}\right)=k\left(\frac{1}{n}\right)$，即

$$\tau:\left(\frac{1}{n}\right)\to k\left(\frac{1}{n}\right). \tag{3}$$

对于$\frac{m}{n}\in A$，其中 m,n 是正整数，由 τ 保持运算及(3)，有

$$\tau:\frac{m}{n}=\underbrace{\frac{1}{n}+\frac{1}{n}+\cdots+\frac{1}{n}}_{m\text{个}}\rightarrow\underbrace{k\left(\frac{1}{n}\right)+k\left(\frac{1}{n}\right)+\cdots+k\left(\frac{1}{n}\right)}_{m\text{个}}=mk\left(\frac{1}{n}\right)=k\left(\frac{m}{n}\right).\qquad(4)$$

对于$-\frac{m}{n}\in A$，其中m,n是正整数，由τ保持运算及(4)，有

$$\tau:\frac{m}{n}+\left(-\frac{m}{n}\right)\rightarrow k\left(\frac{m}{n}\right)+\tau\left(-\frac{m}{n}\right).$$

又由(1)，有

$$\tau:\frac{m}{n}+\left(-\frac{m}{n}\right)=0\rightarrow 0.$$

而τ是映射，从而$k\left(\frac{m}{n}\right)+\tau\left(-\frac{m}{n}\right)=0$，于是$\tau\left(-\frac{m}{n}\right)=-k\left(\frac{m}{n}\right)$，即

$$\tau:-\frac{m}{n}\rightarrow k\left(-\frac{m}{n}\right).\qquad(5)$$

由(1)，(4)，(5)，$\forall x\in A$，都有

$$\tau:x\rightarrow kx,$$

这里k是一个不等于零的有理数．又τ是A的任意一个对于普通加法来说的自同构，从而命题得证．

8. $A=\{$所有有理数$\}$；A的代数运算是普通加法．$\bar{A}=\{$所有不等于零的有理数$\}$；$\bar{A}$的代数运算是普通乘法．证明：对于所给的代数运算来说，A与$\bar{A}$间没有同构映射存在(先决定0在一个同构映射之下的象)．

证一　(反证法)设A与$\bar{A}$间存在同构映射：

$$\phi:a\rightarrow\bar{a}.$$

设

$$\phi:0\rightarrow\bar{0}.$$

因ϕ保持运算，故

$$\phi:a+0\rightarrow\bar{a}\,\bar{0}.$$

又因$a+0=a$，且ϕ是A到$\bar{A}$的映射，故$\bar{a}\,\bar{0}=\bar{a}$．因$\bar{a}\in\bar{A}$，故$\bar{a}\neq 0$，从而$\bar{0}=1$，即

$$\phi:0\rightarrow 1.\qquad(1)$$

对于$-1\in\bar{A}$，因ϕ是A到$\bar{A}$的满射，故$\exists x\in A$，使得

$$\phi:x\rightarrow -1.$$

因ϕ保持运算，故

$$\phi:2x=x+x\rightarrow(-1)(-1)=1.$$

因ϕ是A到$\bar{A}$的单射，故由(1)有$2x=0$，从而$x=0$，即

$$\phi:0\rightarrow -1.\qquad(2)$$

因ϕ是A到$\bar{A}$的映射，故由(1)，(2)，$1=-1$，此为不可能．所以A与$\bar{A}$间没有同构映射．

证二　(反证法)若A与$\bar{A}$间有同构映射ϕ，设$\phi(0)=\bar{0}$．由ϕ保持运算，有

$$\phi(0)=\phi(0+0)=\phi(0)\phi(0)=\bar{0}\,\bar{0}=\bar{0}^2.$$

又由ϕ是单射，有$\bar{0}=\bar{0}^2$，从而$\bar{0}^2-\bar{0}=\bar{0}(\bar{0}-1)=0$．但$\bar{0}\in\bar{A}$，因此$\bar{0}\neq 0$．于是有$\bar{0}=1$，即$\phi(0)=1$．

对于 $-1\in\overline{A}$，因 ϕ 是满射，故 $\exists x\in A$，使得 $\phi(x)=-1$. 因 ϕ 保持运算，故 $\phi\big(x+(-x)\big)=\phi(x)\phi(-x)$. 由 $\phi(0)=1,\phi(x)=-1$，得 $1=-\phi(-x)$，即 $\phi(-x)=-1$. 又 ϕ 是单射，从而 $x=-x$，即 $2x=0,x=0$，于是 $\phi(0)=-1$. 因 ϕ 是映射，又 $\phi(0)=1$，故 $-1=1$，此为不可能．所以 A 与 $\overline{A}$ 间没有同构映射.

证三 (反证法)设 A 与 $\overline{A}$ 间有同构映射

$$\phi: a\to\bar{a}.$$

因 ϕ 保持运算，故

$$\phi: 2a=a+a\to\bar{a}\,\bar{a}=\bar{a}^2.$$

因 $\bar{a}\in\overline{A}$，故 $-\bar{a}\in\overline{A}$. 又 ϕ 是满射，因此 $\exists b\in A$，使得

$$\phi: b\to-\bar{a}.$$

因 ϕ 保持运算，故

$$\phi: 2b=b+b\to(-\bar{a})(-\bar{a})=\bar{a}^2.$$

因 ϕ 是单射，故 $2a=2b$，从而 $a=b$，即

$$\phi: a\to-\bar{a}.$$

因 ϕ 是映射，故 $\bar{a}=-\bar{a}$，于是 $2\bar{a}=0,\bar{a}=0$，此与 $\bar{a}\in\overline{A}$ 矛盾．所以 A 与 $\overline{A}$ 间没有同构映射.

证四 (反证法)设 A 与 $\overline{A}$ 间有同构映射 ϕ．对于 $2\in\overline{A}$，因 ϕ 是满射，故 $\exists a\in A$，使得

$$\phi: a\to 2.$$

因 ϕ 保持运算，故

$$\phi: 2a=a+a\to 2\cdot 2=4.$$

对于 $-2\in\overline{A}$，因 ϕ 是满射，故 $\exists b\in A$，使得

$$\phi: b\to-2.$$

因 ϕ 保持运算，故

$$\phi: 2b=b+b\to(-2)(-2)=4.$$

因 ϕ 是单射，故 $2a=2b$，从而 $a=b$，即

$$\phi: a\to-2.$$

由 ϕ 是映射及 $\phi: a\to 2$，得 $2=-2$，此为不可能．所以 A 与 $\overline{A}$ 间没有同构映射.

证五 (反证法)设 A 与 $\overline{A}$ 间有同构映射 ϕ．对于 $2\in\overline{A}$，因 ϕ 是满射，故 $\exists a\in A$，使得

$$\phi: a\to 2.$$

因 ϕ 保持运算，故

$$\phi: a=\frac{a}{2}+\frac{a}{2}\to\phi\left(\frac{a}{2}\right)\phi\left(\frac{a}{2}\right)=\phi^2\left(\frac{a}{2}\right).$$

因 ϕ 是映射，故 $\phi^2\left(\frac{a}{2}\right)=2$，从而 $\phi\left(\frac{a}{2}\right)=\pm\sqrt{2}$. 但 $\pm\sqrt{2}$ 是无理数，因此 $\phi\left(\frac{a}{2}\right)\overline{\in}\,\overline{A}$. 而 $\frac{a}{2}\in A$，此与 ϕ 是 A 到 $\overline{A}$ 的映射矛盾．所以 A 与 $\overline{A}$ 间没有同构映射.

证六 (反证法)设 A 与 $\overline{A}$ 间有同构映射 ϕ，则 $\forall a\in A$，

$$\phi: a=\frac{a}{2}+\frac{a}{2}\to\phi\left(\frac{a}{2}\right)\phi\left(\frac{a}{2}\right)=\phi^2\left(\frac{a}{2}\right)>0.$$

因而 A 中任意元在 ϕ 下的象都是正有理数，$\overline{A}$ 中的负有理数在 ϕ 下没有逆象，此与 ϕ 是

A 到 $\overline{A}$ 的满射矛盾．所以 A 与 $\overline{A}$ 间没有同构映射.

注　1)　在该命题的已知条件下，A 到 $\overline{A}$ 也没有同态满射存在.

2)　把 $\overline{A}$ 改为有理数集，该命题仍然成立.

3)　要证明 A 与 $\overline{A}$ 间不存在同构映射，这就需要证明 A 到 $\overline{A}$ 的任一映射都不是同构映射，要想逐一验证显然是很困难的．因此证明两个代数系统不同构，一般都用反证法，而且推导时要特别注意特殊元素的象与逆象．有时还可分析这两个代数系统的代数性质是否有明显的差异，根据同构的性质来证明．比如 A 的代数运算"$\circ$"适合交换律，而 $\overline{A}$ 的代数运算"$\bar{\circ}$"不适合交换律，则显然 A 与 $\overline{A}$ 不同构．

三、讲与练

1. 证明：ϕ是 A 与 $\overline{A}$ 间的一个一一映射

$\Leftrightarrow \phi^{-1}: \forall \bar{a}\in\overline{A}, \bar{a}\to\phi^{-1}(\bar{a})=a$，若$\phi(a)=\bar{a}$，是 $\overline{A}$ 与 A 间的一个一一映射.

证　($\Rightarrow$)

1)　ϕ^{-1}是 $\overline{A}$ 到 A 的一个映射．事实上，$\forall \bar{a}\in\overline{A}$，因$\phi$是满射，故 $\exists a\in A$，使得$\phi(a)=\bar{a}$. 同时ϕ又是单射，从而 $\exists| a\in A$，使得$\phi(a)=\bar{a}$. 所以 $\exists| a\in A$，使得$\phi^{-1}(\bar{a})=a$.

2)　ϕ^{-1}是 $\overline{A}$ 到 A 的一个满射．事实上，$\forall a\in A$，因ϕ是映射，故 $\exists \bar{a}\in\overline{A}$，使得$\phi(a)=\bar{a}$，即$\phi^{-1}(\bar{a})=a$.

3)　ϕ^{-1}是 $\overline{A}$ 到 A 的一个单射．事实上，$\forall \bar{a},\bar{b}\in\overline{A}$，若$\phi^{-1}(\bar{a})=\phi^{-1}(\bar{b})=x$，则$\phi(x)=\bar{a}$，$\phi(x)=\bar{b}$. 因$\phi$是映射，故 x 在ϕ下的象唯一，从而 $\bar{a}=\bar{b}$.

因此，ϕ^{-1}是 $\overline{A}$ 与 A 间的一个一一映射.

($\Leftarrow$)

1)　ϕ是 A 到 $\overline{A}$ 的一个映射．事实上，$\forall a\in A$，因ϕ^{-1}是满射和单射，故 $\exists| \bar{a}\in\overline{A}$，使得$\phi^{-1}(\bar{a})=a$，从而 $\exists| \bar{a}\in\overline{A}$，使得$\phi(a)=\bar{a}$.

2)　ϕ是 A 到 $\overline{A}$ 的一个满射．事实上，$\forall \bar{a}\in\overline{A}$，因$\phi^{-1}$是映射，故 $\exists a\in A$，使得$\phi^{-1}(\bar{a})=a$，从而 $\exists a\in A$，使得$\phi(a)=\bar{a}$.

3)　ϕ是 A 到 $\overline{A}$ 的一个单射．事实上，$\forall a,b\in A$，若$\phi(a)=\phi(b)=\bar{x}$，则$\phi^{-1}(\bar{x})=a$，$\phi^{-1}(\bar{x})=b$. 因ϕ^{-1}是映射，故 $a=b$.

所以，ϕ是 A 与 $\overline{A}$ 间的一个一一映射.

注　1)　上面命题很重要．不仅结论很有用，而且其证明是一个很好的基本训练．请读者先不看本书，严格按定义独立给出详细证明.

2)　这里要特别强调：$\bar{a}(\in\overline{A})$在ϕ^{-1}下的象是 $\bar{a}(\in\overline{A})$在ϕ下的逆象，即

$$\phi^{-1}(\bar{a})=a\Leftrightarrow\phi(a)=\bar{a}.$$

3)　ϕ^{-1}叫做ϕ的逆映射.

4)　由此命题知：判断一个映射ϕ是否存在逆映射，可以通过判断ϕ是否一一映射来确定.

2. 证明：若ϕ是对于$\circ$与$\bar{\circ}$来说，A 与 $\overline{A}$ 间的一个同构映射，则ϕ的逆映射ϕ^{-1}是对于$\bar{\circ}$与$\circ$来说，$\overline{A}$ 与 A 间的一个同构映射．反之也成立．即

$$A \overset{\phi}{\cong} \overline{A} \Leftrightarrow \overline{A} \overset{\phi^{-1}}{\cong} A.$$

证 （$\Rightarrow$） 由前一命题知

$$\phi^{-1}: \bar{a} \to \phi^{-1}(\bar{a}) = a, \quad 若\phi(a) = \bar{a}$$

是 $\overline{A}$ 与 A 间的一个一一映射．$\forall \bar{a}, \bar{b} \in \overline{A}$，

$$\phi^{-1}: \bar{a} \to a, 若\phi(a) = \bar{a},$$

$$\phi^{-1}: \bar{b} \to b, 若\phi(b) = \bar{b}.$$

因 ϕ 是 A 与 $\overline{A}$ 间的同构映射，故

$$\phi(a \circ b) = \phi(a) \bar{\circ} \phi(b) = \bar{a} \bar{\circ} \bar{b},$$

从而

$$\phi^{-1}(\bar{a} \bar{\circ} \bar{b}) = a \circ b.$$

所以 ϕ^{-1} 保持运算，于是

$$\overline{A} \overset{\phi^{-1}}{\cong} A.$$

（$\Leftarrow$） 由前一命题知 ϕ 是 A 与 $\overline{A}$ 间的一个一一映射．$\forall a, b \in A$，

$$\phi: a \to \bar{a}, \quad b \to \bar{b},$$

从而

$$\phi^{-1}(\bar{a}) = a, \quad \phi^{-1}(\bar{b}) = b.$$

因 ϕ^{-1} 是 $\overline{A}$ 与 A 间的同构映射，故

$$\phi^{-1}(\bar{a} \bar{\circ} \bar{b}) = \phi^{-1}(\bar{a}) \circ \phi^{-1}(\bar{b}) = a \circ b,$$

从而

$$\phi(a \circ b) = \bar{a} \bar{\circ} \bar{b}.$$

所以

$$A \overset{\phi}{\cong} \overline{A}.$$

3. 证明：

$$A 是有限集 \Leftrightarrow A 与其任一真子集间不存在一一映射.$$

证 （$\Rightarrow$） （反证法）设 $\overline{A}$ 是 A 的任一真子集，且 A 与 $\overline{A}$ 分别含有 n 与 m 个元．若 A 与 $\overline{A}$ 间有一一映射 ϕ，则因 ϕ 是单射，故 A 中的不同元在 ϕ 下必有象，且象也不同，从而 $n \leqslant m$，此与 $\overline{A}$ 是 A 的真子集矛盾．

（$\Leftarrow$） （反证法）若 A 是无限集．取 $a_1 \in A$，因 A 是无限集，故 $A - \{a_1\} \neq \varnothing$，可取 $a_2 \in A - \{a_1\}$．同理 $A - \{a_1, a_2\} \neq \varnothing$，可取 $a_3 \in A - \{a_1, a_2\}$，这样继续取出

$$a_1, a_2, a_3, \cdots, a_n, \cdots$$

因 A 是无限集，于是得一无限集合

$$B = \{a_1, a_2, a_3, \cdots, a_n, \cdots\}.$$

B 是 A 的子集，但未必是真子集．令 $C = A - B$. 再作集合 $D = \{a_2, a_4, a_6, \cdots\}$，则 D 是 B 的真子集，从而 D 也是 A 的真子集，进而 D 的元与 C 的元作成的集合 $\overline{A} = D \cup C$ 也是 A 的真子集．作

$$\phi: a_1 \to a_2,$$

$$a_2 \rightarrow a_4,$$
$$a_3 \rightarrow a_6,$$
$$\vdots \quad \vdots$$
$$a_n \rightarrow a_{2n}.$$

$n=1,2,3,\cdots,\forall a\in C$,

$$\phi: a \rightarrow a.$$

则ϕ是 A 与其真子集$\overline{A}$ 间的一个一一映射．此与题设矛盾．

注　1)　必要性($\Rightarrow$)的另一证法．设$\overline{A}$是A的任一真子集．

①　若$\overline{A}=\varnothing$，因$A\neq\overline{A}$，故$A\neq\varnothing$，于是$\exists a\in A$，但在$\overline{A}$中没有元素作为a的象，所以不存在A到$\overline{A}$的映射．

②　若$\overline{A}\neq\varnothing$，设$\overline{A}=\{a_1,a_2,\cdots,a_n\}$，我们对$n$用数学归纳法证明$A$与$\overline{A}$间不存在一一映射．

(i)　$n=1$时，$\overline{A}=\{a_1\}$．如果A与$\overline{A}$间存在一一映射ϕ．因$\overline{A}\subset A$，故$a_1\in A$．又$A\neq\overline{A}$，故还$\exists a_2\in A$，而$a_2\neq a_1$．因ϕ是A到$\overline{A}$的映射，故对于$a_1,a_2\in A$，有

$$\phi(a_1)=a_1,\ \phi(a_2)=a_1.$$

此与ϕ是A到$\overline{A}$的单射矛盾．所以$n=1$时命题成立．

(ii)　假定$n-1$时，A与其任意一个含$n-1$个元素的真子集间不存在一一映射．今证n时，A与其任意一个含n个元素的真子集$\overline{A}=\{a_1,a_2,\cdots,a_n\}$间也不存在一一映射．

不然，如果A与$\overline{A}=\{a_1,a_2,\cdots,a_n\}$间存在一一映射$\phi$．因$\overline{A}\subset A$，故$a_1,a_2,\cdots,a_n\in A$．又$A\neq\overline{A}$，故还$\exists a_{n+1}\in A$，而$a_{n+1}\neq a_i$，$i=1,2,\cdots,n$．因$\phi$是$A$到$\overline{A}$的映射．故对于$a_{n+1}\in A$，$\exists a_t\in\overline{A}$，使得$\phi(a_{n+1})=a_t$，$1\leqslant t\leqslant n$．于是$\phi$是$A-\{a_{n+1}\}$与$\overline{A}-\{a_t\}$间的一一映射．而且我们可以断言，$\overline{A}-\{a_t\}$是$A-\{a_{n+1}\}$的真子集．事实上，因$\overline{A}\subset A$，故$a_1,a_2,\cdots,a_{t-1},a_{t+1},\cdots,a_n\in A$．又因$a_{n+1}\neq a_i$，$i=1,2,\cdots,n$，故$a_1,a_2,\cdots,a_{t-1},a_{t+1},\cdots,a_n\in A-\{a_{n+1}\}$，即$\overline{A}-\{a_t\}\subset A-\{a_{n+1}\}$．因$a_t\in A-\{a_{n+1}\}$，但$a_t\overline{\in}\overline{A}-\{a_t\}$，故$\overline{A}-\{a_t\}$是$A-\{a_{n+1}\}$的真子集．此与归纳假定矛盾．于是$n$时，$A$与其任一含$n$个元素的真子集$\overline{A}$间也不存在一一映射．

由归纳原理，命题得证．

2)　无限集必与其某一个真子集间可以建立一一映射，这是有限集与无限集的本质区别，是有限集与无限集相互区别的一个特征性质．因此有的教科书上这样给出定义：若集合A有真子集$\overline{A}$使A与$\overline{A}$间存在一一映射，则称A为无限集．否则，若集合A没有真子集$\overline{A}$使A与$\overline{A}$间存在一一映射，则称A为有限集．

4. (鸽笼定理)设A与$\overline{A}$都是有限集，且含有相同个数的元素，又ϕ是A到$\overline{A}$的一个映射．证明：

1)　若ϕ为单射，则ϕ必为满射；

2)　若ϕ为满射，则ϕ必为单射．

证　(反证法)

1)　假定ϕ不是满射，则$\exists\overline{y}\in\overline{A}$，$\overline{y}$在$\phi$下无逆象在$A$中，于是在$\overline{A}$中作为象的元的个数小于$A$中的元的个数．又$\phi$是映射，$A$与$\overline{A}$含有相同个数的元素．因此，在$A$中必至少有两个不同的元映到$\overline{A}$中的同一个元．此与$\phi$是单射矛盾，从而$\phi$是满射．

2) 假定ϕ不是单射,则在 A 中有两个不同的元在$\overline{A}$ 中有同一个象．又ϕ是映射,$\overline{A}$ 与 A 含有相同个数的元素,从而在 $\overline{A}$ 中作为象的元的个数小于$\overline{A}$ 中的元的个数．因此,在 $\overline{A}$ 中存在无逆象的元,于是ϕ不是满射．此与已知矛盾．所以ϕ是单射.

注 由鸽笼定理,可以解决下面问题.

设 $A=\{1,2,3\}$,ϕ是 A 到 A 的满射,且$\phi(1)=3$. 求ϕ的个数.

解 由鸽笼定理,ϕ必为 A 到 A 的单射．因此,ϕ是 A 与 A 间的一个一一映射.

今$\phi(1)=3$,从而ϕ有且只有$(3-1)!=2!=2$种可能,即

$$1\to 3,\ 2\to 1,\ 3\to 2,$$

或

$$1\to 3,\ 2\to 2,\ 3\to 1.$$

一般来说,

设 $A=\{1,2,\cdots,n\}$,ϕ是 A 到 A 的满射,且$\phi(i)=j_i$,$i=1,2,\cdots,k$,$k<n$,这里 $j_i(i=1,2,\cdots,k)$是 A 中固定的 k 个元．则这样的ϕ的个数是$(n-k)!$.

证 由鸽笼定理,ϕ是 A 与 A 间的一个一一映射．今限定$\phi(i)=j_i$,$i=1,2,\cdots,k$,$k<n$. 因此,只需确定 A 中 $n-k$ 个元:$k+1,\cdots,n$ 在一一映射ϕ下的象．即

$$\begin{aligned}A&=\{1,2,\cdots,k,k+1,\cdots,n\}\\&=\{j_1,j_2,\cdots,j_k,j_{k+1},\cdots,j_n\}.\end{aligned}$$

而

$$\phi(k+l)=j_{k+r}.\quad 1\leqslant l,r\leqslant n-k.$$

所以,ϕ的个数应为 $n-k$ 个元素的全排列数$(n-k)!$.

5. 设$\mathbf{R}$是实数集,a,b,c 是任意给定的三个实数,$F=\left\{y\,\middle|\,y=ax^2+bx+c,x\in\mathbf{R}\right\}$,

$$\phi:x\to\phi(x)=y=ax^2+bx+c.$$

证明:ϕ是$\mathbf{R}$到 F 的一个满射．ϕ是否为$\mathbf{R}$到 F 的单射呢?

证 1) $\forall x\in\mathbf{R}$,$\exists|\,y=ax^2+bx+c\in F$,从而$\phi$是$\mathbf{R}$到 F 的映射.

2) $\forall y=ax^2+bx+c\in F$,$\exists x\in\mathbf{R}$,使得

$$\phi(x)=y.$$

所以ϕ是$\mathbf{R}$到 F 的满射.

下面讨论ϕ是否为$\mathbf{R}$到 F 的单射.

1) 当 $a\neq 0$ 时,

① 若 $b\neq 0$,取 $x_1=0$,$x_2=-\dfrac{b}{a}\in\mathbf{R}$,显然 $x_1\neq x_2$. 但$\phi(x_1)=\phi(x_2)=c$,从而ϕ不是$\mathbf{R}$到 F 的单射.

② 若 $b=0$,取 $x_1=1$,$x_2=-1$,显然 $x_1\neq x_2$. 但$\phi(x_1)=\phi(x_2)=a+c$,从而ϕ不是$\mathbf{R}$到 F 的单射.

2) 当 $a=0$ 时,

① 若 $b\neq 0$,$y=bx+c$,显然当 $x_1\neq x_2$ 时,有 $bx_1+c\neq bx_2+c$,从而ϕ是$\mathbf{R}$到 F 的单射.

② 若 $b=0$,$y=c$,不论 x 为何实数,y 都是 c,从而ϕ不是$\mathbf{R}$到 F 的单射.

6. 设 n 是固定的自然数,ϕ是自然数集$\mathbf{N}$的变换,

$$\phi(k)=\begin{cases} n-k(k<n), \\ n+k(k\geqslant n). \end{cases}$$

问ϕ是否为$\mathbb{N}$的单射变换？满射变换？

解　$\forall k,l\in\mathbb{N}$.

1)　若$k<n$,且$l<n$,$\phi(k)=n-k=n-l=\phi(l)$时,有$k=l$.

2)　若$k\geqslant n$,且$l\geqslant n$,$\phi(k)=n+k=n+l=\phi(l)$时,有$k=l$.

3)　若$k<n$,$l\geqslant n$,则$\phi(l)=n+l$,$\phi(k)=n-k$. 因$l>k$,故$n+l>n+k$. 又$k>0$,从而$k>-k$,所以$n+k>n-k$. 于是$n+l>n-k$,即$\phi(l)\neq\phi(k)$.

综上知ϕ是$\mathbb{N}$的单射变换.

ϕ不是$\mathbb{N}$的满射变换．事实上,取$n\in\mathbb{N}$,若n在ϕ下在$\mathbb{N}$中有逆象,则$n=n-k$或$n=n+k$. 此时必有$k=0$,此与$k\in\mathbb{N}$矛盾．故n在ϕ下在$\mathbb{N}$中无逆象.

注　1)　特别注意,不能因$\forall n-k\in\mathbb{N}$,$\exists k\in\mathbb{N}$,使得$\phi(k)=n-k$,且$\forall n+k\in\mathbb{N}$,$\exists k\in\mathbb{N}$,使得$\phi(k)=n+k$,就下结论说ϕ是$\mathbb{N}$的满射变换．必须对于$\mathbb{N}$中的任意一个元l,在ϕ下在$\mathbb{N}$中都有逆象,才能说ϕ是$\mathbb{N}$的满射变换.

2)　该题中,$\mathbb{N}$的所有的元在ϕ下的象的全体是$\mathbb{N}-\{n,n+1,\cdots,n+(n-1)\}$.

7. 设A,B,C是集合K的三个子集,且$A=B\cup C$,$B\cap C=\varnothing$. 将A的全部子集作成的集合记为$P(A)$,B的全部子集作成的集合记为$P(B)$,C的全部子集作成的集合记为$P(C)$. 试找出$P(A)$与卡氏积$P(B)\times P(C)$间的一个一一映射.

解一　$\forall S\in P(A)$,作法则

$$\phi: S\rightarrow(S\cap B,S\cap C).$$

则ϕ是$P(A)$与$P(B)\times P(C)$间的一个一一映射．事实上,

1)　ϕ显然是映射.

2)　ϕ是单射．因为:$\forall S,T\in P(A)$,若$\phi(S)=(S\cap B,S\cap C)=(T\cap B,T\cap C)=\phi(T)$,则$S\cap B=T\cap B$,$S\cap C=T\cap C$. 又

$$(S\cap B)\cup(S\cap C)=S\cap(B\cup C)=S\cap A=S,$$
$$(T\cap B)\cup(T\cap C)=T\cap(B\cup C)=T\cap A=T,$$

从而$S=T$.

3)　ϕ是满射．因为:$\forall(B_i,C_i)\in P(B)\times P(C)$,其中$B_i\in P(B)$,$C_i\in P(C)$. 记$B_i\cup C_i=A_i$. 因$B_i\cup C_i\subset B\cup C=A$,故$A_i\in P(A)$. 又$\phi(A_i)=(A_i\cap B,A_i\cap C)$,已知$C\cap B=\varnothing$,因此$A_i\cap B=(B_i\cup C_i)\cap B=(B_i\cap B)\cup(C_i\cap B)=B_i\cup\varnothing=B_i$. 同理,$A_i\cap C=C_i$,从而$\exists A_i\in P(A)$,使得$\phi(A_i)=(B_i,C_i)$.

所以,ϕ是$P(A)$与$P(B)\times P(C)$间的一个一一映射.

解二　$\forall S\in P(A)$,有$S\subset A=B\cup C$. 因此,$\exists B_i\subset B$,$C_i\subset C$,使得$S=B_i\cup C_i$. 令

$$\phi: S\rightarrow(B_i,C_i),$$

则ϕ是$P(A)$与$P(B)\times P(C)$间的一个一一映射．事实上,

1)　ϕ是映射．$\forall S\in P(A)$,$\exists(B_i,C_i)\in P(B)\times P(C)$,$S=B_i\cup C_i$,使得$\phi(S)=(B_i,C_i)$,且$S=B_i\cup C_i$的表法唯一(若还有$S=B_j\cup C_j$,$B_j\in P(B)$,$C_j\in P(C)$,则$B_i\cup C_i=B_j\cup C_j\Rightarrow B_i\cup C_i-B_j-C_i=B_j\cup C_j-B_j-C_i\Rightarrow B_i-B_j=C_j-C_i$. 但$B_i-B_j\in P(B)$,$C_j-C_i\in P(C)$,又$B\cap C=\varnothing$,从而由$B_i-B_j\in B\cap C$,$C_j-C_i\in B\cap C$,得$B_i-B_j=C_j-C_i=\varnothing$

$\Rightarrow B_i=B_j, C_i=C_j$). 因此，$\exists!(B_i,C_i)\in P(B)\times P(C)$，使得$\phi(S)=(B_i,C_i)$.

2) ϕ是单射．因为：$\forall S,T\in P(A)$，若$\phi(S)=(B_i,C_i)=(B_j,C_j)=\phi(T)$，其中 $S=B_i\cup C_i, T=B_j\cup C_j$，则 $B_i=B_j, C_i=C_j$，从而 $S=T$.

3) ϕ是满射．因为：$\forall(B_i,C_i)\in P(B)\times P(C)$，$\exists A_i=B_i\cup C_i$. 因 $B_i\cup C_i\subset B\cup C=A$，故 $A_i\in P(A)$，且$\phi(A_i)=(B_i,C_i)$.

所以，ϕ是 $P(A)$与 $P(B)\times P(C)$间的一个一一映射.

8. 设$\mathbb{Z}$是整数集，$\mathbb{Z}$的代数运算是普通乘法．$\mathbb{Z}_0$是偶数集，$\mathbb{Z}_0$的代数运算是普通乘法. 证明：对于所给的代数运算来说，$\mathbb{Z}$与$\mathbb{Z}_0$不同构．

证　(反证法)若$\mathbb{Z}\cong\mathbb{Z}_0$，则存在$\mathbb{Z}$与$\mathbb{Z}_0$间的一个同构映射，设为$\phi$．又设

$$\phi:1\to a.$$

由ϕ保持运算，有

$$\phi:1\cdot 1\to a\cdot a.$$

由 $1=1\cdot 1$，ϕ是映射，有 $a=a\cdot a=a^2\Rightarrow a^2-a=0\Rightarrow a(a-1)=0$. 因 $a\in\mathbb{Z}_0$，故 $a\neq 1$，从而$a=0$，即

$$\phi:1\to 0.$$

设

$$\phi:2\to b.$$

由ϕ保持运算，有

$$\phi:1\cdot 2=2\to 0\cdot b=0.$$

但ϕ是单射，0 在ϕ下的逆象唯一，即 $1=2$，此为不可能，故$\mathbb{Z}\ncong\mathbb{Z}_0$.

四、思考问题

1. 设 $A=\left\{n\,\middle|\,n<5, n\in\mathbb{N}\right\}$，$B=\left\{n\,\middle|\,n\leqslant 5, n\in\mathbb{N}\right\}$.

1) 写出一个 A 到 B 的映射，但不是单射.

2) 写出一个 A 到 B 的单射.

3) 是否存在 A 到 B 的满射？

4) 写出一个 B 到 A 的映射，但不是满射.

5) 写出一个 B 到 A 的满射.

6) 是否存在 B 到 A 的单射？

2. 以下各法则ϕ是否为 A 到 B 的满射？单射？

1) A 表示某四年制大学数学系全体学生所作成的集合，$B=\{1,2,3,4\}$.

$$\phi:a\to a\text{ 所在的年级}.$$

2) $A=\{$某班学生$\}$，$B=$实数集.

$$\phi:x\to x\text{ 的年龄}.$$

3) $A=B=$实数集.

$$\phi:x\to x^4.$$

4) $A=B=$自然数集.

$$\phi: x \to x^2+1.$$

5)　A=整数集，$B=\left\{4x^2+1 \middle| x\in A\right\}$.

$$\phi: x \to 4x^2+1.$$

6)　A=有理数集，B=非负有理数集.

$$\phi: x \to \frac{1}{x^2+1}.$$

7)　$A=B$=整数集．n 是取定的正整数，

$$\phi: a \to r,$$

其中 r 是 a 被 n 除所得的余数，即 $a=nq+r, 0\leqslant r<n$.

8)　A=整数集，B=正整数集．

$$\phi: n \to |n|.$$

9)　$A=B$=整数集.

$$\phi: \begin{cases} 2n \to n, \\ 2n+1 \to 2n+1. \end{cases}$$

10)　A=实数集，B 是实数域上的一元多项式环.

$$\phi: f(x) \to f(0).$$

11)　A 是 n 阶实对称矩阵的集合，B 是实数域上的 n 维向量空间．取定 B 的一个基 $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n$，$\forall X\in A$，设 X 的主对角线上的元为 $a_1, a_2, \cdots, a_n$，

$$\phi: X \to a_1\varepsilon_1+a_2\varepsilon_2+\cdots+a_n\varepsilon_n.$$

3. 集 A 有 k 个元，集 B 有 n 个元，$k\leqslant n$，求 A 到 B 的单射的个数.

4. 证明下面 A 到 B 的映射 ϕ 是 A 与 B 间的一一映射：

1)　A 与 B 都是闭区间[0,1]上全体实函数 $f(x)$ 作成的集合.

$$\phi: f(x) \to (x^2+1)f(x).$$

2)　A 是整数集，B 是非负整数集.

$$\phi: \begin{cases} n \to 2n, & \text{当 } n\geqslant 0 \text{ 时}, \\ n \to -2n-1, & \text{当 } n<0 \text{ 时}. \end{cases}$$

5. 试建立下面 A 与 $\overline{A}$ 间的一一映射.

1)　$A=\left\{x \middle| x \text{ 是小于 100 的正奇数}\right\}$，$\overline{A}=\left\{\overline{x} \middle| \overline{x} \text{ 是不大于 100 的正偶数}\right\}$.

2)　A 是自然数集，$\overline{A}$ 是非负整数集.

3)　A={所有大于或等于零的整数}，$\overline{A}$={所有大于零的整数}.

4)　A={所有大于或等于零的实数}，$\overline{A}$={所有大于零的实数}.

5)　$X=\{x_1, x_2, \cdots, x_n, \cdots\}$，$Y=\{y_1, y_2, \cdots, y_n, \cdots\}$，且 $X\cap Y=\varnothing$，$A=X\cup Y$，$\overline{A}$=自然数集.

6)　A 是整数集，$\overline{A}$ 是自然数集.

7)　A 是正实数集，$\overline{A}$ 是开区间(0,1).

8)　A 是正实数集，$\overline{A}$ 是开区间(−1,0).

6. 试求下面 A 与 $\overline{A}$ 间的一一映射 ϕ 的逆映射 ϕ^{-1}：

1)　$A=\overline{A}$=实数集.

$$\phi: x \to 2x+1.$$

2) $A=\{$所有 n 行 m 列矩阵$\}$, $\bar{A}=\{$所有 m 行 n 列矩阵$\}$.

$$\phi: X \to X',$$

其中 X' 是 n 行 m 列矩阵 X 的转置矩阵.

3) $A=(-\infty,0]$, $\bar{A}=[0,+\infty)$.

$$\phi: x \to x^2.$$

4) $A=[a,b]$, $\bar{A}=[c,d]$, $a<b$, $c<d$.

$$\phi: x \to \frac{d-c}{b-a}(x-a)+c.$$

7. 证明:对于下列各代数运算$\circ$和$\bar{\circ}$来说,A 与 $\bar{A}$ 同态.

1) $A=$整数集,$\circ$是普通乘法,$\bar{A}=\{-1,0,1\}$,$\bar{\circ}$是普通乘法.

2) $A=$复数集,$\circ$是普通加法,$\bar{A}=$实数集,$\bar{\circ}$是普通加法.

3) $A=\{1,\mathrm{i},-1,-\mathrm{i}\}$,$\circ$是普通乘法,$\bar{A}=\{1,-1\}$,$\bar{\circ}$是普通乘法.

4) $A=$有理数集,$\circ$是普通乘法,$\bar{A}=$整数集,$\bar{\circ}$是普通加法.

8. 证明:

$$\phi: m+n\sqrt{2} \to m+n\sqrt{3}$$

不是 $A=\left\{m+n\sqrt{2}\,\middle|\,m,n\in\mathbb{Z}\right\}$ 与 $\bar{A}=\left\{m+n\sqrt{3}\,\middle|\,m,n\in\mathbb{Z}\right\}$ 间的对于一对普通乘法来说的同构映射.

9. 证明:对于下面所给的各代数运算$\circ$与$\bar{\circ}$来说,A 与 $\bar{A}$ 不同构.

1) A 是有理数集,$\circ$是普通加法.$\bar{A}$ 是整数集,$\bar{\circ}$是普通加法.

2) A 是非零实数集,$\circ$是普通乘法.$\bar{A}$ 是实数集,$\bar{\circ}$是普通加法.

10. 下面各命题对吗?设对于代数运算$\circ$和$\bar{\circ}$来说,$A \overset{\phi}{\sim} \bar{A}$.

1) 若$\bar{\circ}$适合结合律,则$\circ$也适合结合律.

2) 若$\bar{\circ}$适合交换律,则$\circ$也适合交换律.

11. 下面命题对吗?设$\odot$,$\oplus$是集 A 的代数运算,$\bar{\odot}$,$\bar{\oplus}$是集 $\bar{A}$ 的代数运算,且对于$\odot$,$\bar{\odot}$来说,$A \overset{\phi}{\sim} \bar{A}$,对于$\oplus$,$\bar{\oplus}$来说,也有 $A \overset{\phi}{\sim} \bar{A}$.

1) 若$\bar{\odot}$,$\bar{\oplus}$适合第一分配律,则$\odot$,$\oplus$也适合第一分配律.

2) 若$\bar{\odot}$,$\bar{\oplus}$适合第二分配律,则$\odot$,$\oplus$也适合第二分配律.

第三章　等价关系与集合的分类

一、基本问题问答

1. 集合 A 的元间的关系的定义是什么?

答　R 是 A 的元间的一个关系

$$\Leftrightarrow R \text{ 是 } A\times A \text{ 到 } D=\{\text{对},\text{错}\}\text{的一个映射}.$$

$R:(a,b)\rightarrow$ 对(即 $R(a,b)=$对) $\Leftrightarrow a,b$ 符合关系 $R\Leftrightarrow aRb$.

$R:(a,b)\rightarrow$ 错(即 $R(a,b)=$错) $\Leftrightarrow a,b$ 不符合关系 $R\Leftrightarrow a\not{R}b$.

注　这里 D 是一个有且只有两个元素的集合,可令 $D=\{$是,非$\}$或$\{$黑,白$\}$或$\{$上,下$\}$或$\{$有,无$\}$等都可以.只是为了说明 $\forall a,b\in A$,a 与 b 或者符合关系 R,或者不符合关系 R,两者必居且只居其一,没有第三种可能.

2. 为什么要分类?什么叫做集 A 的一个分类?

答　上万的字,按拼音或偏旁分类,才能在字典上查找.分门别类编成电话号码本,才便于查找电话号码.利用人映到人的属相这一映射,可以按属相把人分成十二类.研究动植物要分类;医院看病要分科;商店的商品要分柜……因此,我们研究问题、处理事情常常也要分类.同样,分类也是研究集合的一种重要方法.

设 $A_1,A_2,\cdots$是集 A 的非空子集,则

$A_1,A_2,\cdots$是 A 的一个分类

$\Leftrightarrow$1)　$\forall a\in A,a\in$某 A_i(无遗漏);

2)　$\forall a\in A,a$ 只$\in$某 A_i(无重复)

$\Leftrightarrow$1)　$A=\bigcup A_i$;

2)　$i\neq j$ 时,$A_i\cap A_j=\varnothing$.

把每个 A_i 叫做类.

3. 集 A 的一个分类与 A 的元间的一个等价关系$\sim$是如何相互决定的?

答 1)　已知 A 有一个分类,则此分类决定一个等价关系$\sim$:$\forall a,b\in A$,

$$a\sim b\Leftrightarrow a,b\text{ 同属一类}$$

($a\sim b$ 表示 a 与 b 符合等价关系,也称 a 与 b 等价).

2)　已知 A 有一个等价关系$\sim$,取定 $a\in A$,则此等价关系$\sim$决定包含元素 a 的类

$$[a]=\left\{x\in A\,\middle|\,x\sim a\right\}.$$

$[a]$也称含 a 的等价类.所有这样的类$[a]$,$[b]$,$\cdots$就是 A 的一个分类[①].

---

①　张禾瑞.近世代数基础.北京:高等教育出版社,1978.28.定理 1、定理 2 的证明.

4. 为何等价类中任一元都可作代表？

答

$$\forall b \in [a] \Rightarrow b \sim a,$$

由等价关系、$[a]$及$[b]$的定义知$[b]=[a]$，从而等价类$[a]$也可由其中元素 b 作代表.

5. 设 a,b,n 都是整数，证明：

$$n \mid a-b \Leftrightarrow a,b \text{ 分别被 } n \text{ 除同余}.$$

证 设

$$a = q_1 n + r_1, 0 \leqslant r_1 < n;$$
$$b = q_2 n + r_2, 0 \leqslant r_2 < n.$$

则 $a-b=(q_1-q_2)n+(r_1-r_2), 0\leqslant |r_1-r_2|<n$.

$(\Rightarrow)$

$$n \mid a-b \Rightarrow n \mid r_1-r_2 \Rightarrow n \mid |r_1-r_2|.$$

因 $0\leqslant |r_1-r_2|<n$，故 $|r_1-r_2|=0 \Rightarrow r_1=r_2$.

$(\Leftarrow)$

$$r_1=r_2 \Rightarrow r_1-r_2=0 \Rightarrow n \mid a-b.$$

6. 什么叫做 a 同余 b 模 n？

答

$$\begin{aligned} a \text{ 同余 } b \text{ 模 } n &\Leftrightarrow n \mid a-b \\ &\Leftrightarrow a,b \text{ 分别被 } n \text{ 除同余} \\ &\Leftrightarrow a \equiv b(n). \end{aligned}$$

7. 什么叫做模 n 的剩余类？模 n 的全部剩余类是什么？

答 设 $\mathbb{Z}$ 是整数集，n 是一个固定的正整数. 容易证明

$$a\sim b \Leftrightarrow n \mid a-b \Leftrightarrow a,b \text{ 分别被 } n \text{ 除同余} \Leftrightarrow a\equiv b(n)$$

是 $\mathbb{Z}$ 的元间的一个等价关系. 由此等价关系决定 $\mathbb{Z}$ 的一个分类，其中的类就称为模 n 的剩余类. 因此含 $a(\in \mathbb{Z})$的模 n 的剩余类是

$$\begin{aligned} [a] &= \{x \in \mathbb{Z} \mid x \sim a\} \\ &= \{x \in \mathbb{Z} \mid n \mid x-a\} \\ &= \{x \mid x-a = qn, q \text{ 是整数}\} \\ &= \{qn + a \mid q \text{ 是整数}\} \\ &= \{\cdots, -2n+a, -n+a, a, n+a, 2n+a, \cdots\}. \end{aligned}$$

当然，类$[a]$中的任一元都可作代表，即

$$[a]=[n+a]=[-n+a]=[2n+a]=[-2n+a]=\cdots=[qn+a],$$

这里 q 为任意整数.

模 n 的全部剩余类是

$$[0]=\{qn \mid q \in \mathbb{Z}\}=\{\cdots,-2n,-n,0,n,2n,\cdots\},$$

$[1]=\{qn+1 \mid q\in\mathbb{Z}\}=\{\cdots,-2n+1,-n+1,1,n+1,2n+1,\cdots\}$,

$[2]=\{qn+2 \mid q\in\mathbb{Z}\}=\{\cdots,-2n+2,-n+2,2,n+2,2n+2,\cdots\}$,

……………………………………………………………………

$[n-1]=\{qn+(n-1) \mid q\in\mathbb{Z}\}$

$=\{\cdots,-2n+(n-1),-n+(n-1),n-1,n+(n-1),2n+(n-1),\cdots\}$.

事实上,$[0],[1],[2],\cdots,[n-1]$都是$\mathbb{Z}$的非空子集．$\forall a\in\mathbb{Z}$,a被n除所得的余必为$0,1,2,\cdots,n-1$中的一个.因此a被n除必与$0,1,2,\cdots,n-1$中的一个被n除同余,从而a必与$0,1,2,\cdots,n-1$中的一个等价.所以a必属于$[0],[1],[2],\cdots,[n-1]$中的一个.又$0,1,2,\cdots,n-1$中任意两个不同的整数被n除都不同余,因此$0,1,2,\cdots,n-1$中任意两个不同的整数都不等价,从而$[0],[1],[2],\cdots,[n-1]$中任意两个类的交都是空集.所以,$\forall a\in\mathbb{Z}$,a只属于$[0],[1],[2],\cdots,[n-1]$中的唯一的一个.于是$[0],[1],[2],\cdots,[n-1]$是$\mathbb{Z}$的一个分类,也就是模n的全部剩余类.

当$n=1$时,整个整数集$\mathbb{Z}$成为一类,这是最“粗”的分类.当$n=2$时,$\mathbb{Z}$就分成两类,一类是所有偶数作成的集合,一类是所有奇数作成的集合.

8. 1)　设$[2]$是模3的剩余类,$[2]$中有哪些元?

2)　设$[2]$是模4的剩余类,$[2]$中有哪些元?

答　1)　$[2]=\{x \mid x\sim 2\}=\{x \mid 3\mid x-2\}=\{x \mid x-2=3q,q\in\mathbb{Z}\}=\{2+3q \mid q\in\mathbb{Z}\}=\{\cdots,-7,-4,-1,2,5,8,\cdots\}$.

2)　$[2]=\{x \mid x\sim 2\}=\{x \mid 4\mid x-2\}=\{x \mid x-2=4q,q\in\mathbb{Z}\}=\{2+4q \mid q\in\mathbb{Z}\}=\{\cdots,-10,-6,-2,2,6,10,\cdots\}$.

注　若模不同,则代表元相同的剩余类也不同.

二、典型问题分析

有人说:假如一个关系R适合对称律和推移律,那么它也适合反射律.他的推论方法是:因为R适合对称律,

$$aRb \Rightarrow bRa.$$

因为R适合推移律,

$$aRb,\ bRa \Rightarrow aRa.$$

这个推论方法有什么错误?

解　推论方法错误的实质在于对反射律和对称律的理解不全面.反射律是没有任何条件的,要求对集合A中任一元a,都有aRa,而对称律是有因果关系的,只有在aRb的条件下,才有bRa.在该证明中是对这样的$a\in A$,在具有条件:$\exists b\in A$,使得aRb时,才能推出aRa,于是此a就未必是A中任一元了.在A中可能有使aRb的b不存在的a,于是就推不出aRa了.例如,

设$A=\left\{\pi,\dfrac{\pi}{2}\right\}$,

$$aRb \Leftrightarrow a,b \text{ 互补}.$$

显然 R 是 A 的元间的一个关系，且 R 适合对称律和推移律. 但 π 与 π 不互补，从而 R 不适合反射律. 这就是因为对于 $\pi\in A$ 来说，在 A 中不存在元素 b，使 πRb，因此，即使对称律和推移律都成立，也推不出反射律.

注 1) 做此题前，可先给出一个具体的关系 R，它适合对称律和推移律，但破坏反射律．这种例子很多，我们再给出一些：

① A＝整数集，

$$aRb \Leftrightarrow ab > 0.$$

② $A=\{1,2,4\}$，

$$aRb \Leftrightarrow 4 \mid a+b.$$

③ $A=\{1,2,3\}$，

$$aRb \Leftrightarrow a+b = 2.$$

④ $A=\{a,b,c\}$，$R(a,a)=R(b,b)=$对，$R(c,c)=$错，$R(a,b)=R(b,a)=$对，$R(a,c)=R(c,a)=R(b,c)=R(c,b)=$错.

⑤ $A=\{a,b,c\}$，

$$xRy \Leftrightarrow x\neq a, \text{且 } y\neq a.$$

⑥ A＝实数集，

$$aRb \Leftrightarrow a^2+b^2 = 0.$$

2) 例子说明了由对称律和推移律不能推出反射律，因此，反射律独立于对称律和推移律. 同样，对称律独立于反射律和推移律，推移律独立于反射律和对称律(见本书第 31 页第 4 题). 所以，三律是彼此独立的.

3) 当集 A 含且仅含两个元时，适合反射律和对称律的 A 的元间的一个关系 R 必适合推移律. 事实上，设 $A=\{a,b\}$，R 适合反射律，必有 $R(a,a)=R(b,b)=$对. R 适合对称律，必有 $R(a,b)=R(b,a)=$对或 $R(a,b)=R(b,a)=$错，从而 R 适合推移律.

4) 对于该问题的解中的例子，以下说法是错误的：当 $a=\frac{\pi}{2}$时，因 aRa，故此时 R 适合反射律；当 $a\neq\frac{\pi}{2}$时，因 $a\not R a$，故此时 R 不适合反射律. 所以 R 不一定适合反射律. 这种说法错误的原因，在于没有真正理解反射律. 反射律要求对于任意 $a\in A$，都有 aRa.

5) 设 R 是集 A 的元间的一个关系，则 R 是 A 的元间的一个等价关系

$\Leftrightarrow$ ① $\forall a\in A$，$\exists b\in A$，使得 aRb；

② $\forall a,b\in A$，$aRb\Rightarrow bRa$；

③ $\forall a,b,c\in A$，aRb，$bRc\Rightarrow aRc$.

三、讲与练

1. 1) 下面的法则 R 是否为集 A 的元间的一个关系？

① A＝整数集，$D=\{$对，错$\}$.

$R(a,b)=$对，当 a 与 b 同号时.

$R(a,b)=$错，当 a 与 b 异号时.

② $A=\{1,2,3\}$，$D=\{$对，错$\}$.

$R(a,b)=$对，当 $a+b=2$ 时.

$R(a,b)=$错，当 $a+b=3$ 时.

2）n 元集 A 的关系共有几个？

解 1）① 取 $0,0\in A$，$(0,0)$在 R 下在 D 中无象，从而 R 不是 A 的元间的一个关系.

② 取 $2,3\in A$，$(2,3)$在 R 下在 D 中无象，这是因为 $2+3=5$，从而 R 不是 A 的元间的一个关系.

2）n 元集 A 的关系共有 $2^{n\times n}$ 个.

2. 试判断下面的集 A 的子集是否为 A 的一个分类.

1）A 是实数集，$\cdots,A_{-2},A_{-1},A_0,A_1,A_2,\cdots$ 是 A 的子集，其中 $A_n=(n-1,n)$，$n=0,\pm1,\pm2,\cdots$.

2）A 是实数集，$\cdots,A_{-2},A_{-1},A_0,A_1,A_2,\cdots$ 是 A 的子集，其中 $A_n=[n-1,n+1]$，$n=0,\pm1,\pm2,\cdots$.

解 1）不是. 因为每个整数 $\in A$ 都不在任何一个 A_n 中.

2）不是. 因为整数 $n\in A$ 既在 $A_n=[n-1,n+1]$中，又在 $A_{n+1}=[n+1-1,n+1+1]$中.

3. 设 $A=\{a,b,c,d\}$，试给出 A 的一个等价关系.

解 首先给出 A 的一个分类，

$$A_1=\{a,b,c\},A_2=\{d\}.$$

于是由此分类决定的等价关系～是：

$$x\sim y\Leftrightarrow x,y\in\text{同一类}$$
$$\Leftrightarrow x,y\in A_1\text{ 或 }x,y\in A_2.$$

即

$$a\sim a,a\sim b,a\sim c,b\sim a,b\sim b,$$
$$b\sim c,c\sim a,c\sim b,c\sim a,d\sim d,$$
$$a\nsim d,b\nsim d,c\nsim d,d\nsim a,d\nsim b,d\nsim c.$$

4. 证明等价关系定义中的三条规律的独立性.

证 反射律的独立性在前面的“二、典型问题分析”中已证.

设 $\mathbb{Z}$ 是整数集，则

$$aRb\Leftrightarrow a\,|\,b.$$

是 $\mathbb{Z}$ 的元间的一个关系. 显然 R 适合反射律和推移律，但 R 不适合对称律，从而对称律独立于反射律和推移律.

设 $\mathbb{Z}$ 是整数集，则

$$aRb\Leftrightarrow ab\geqslant 0$$

是 $\mathbb{Z}$ 的元间的一个关系. 显然 R 适合反射律和对称律.

若 aRb,bRc，即 $ab\geqslant0,bc\geqslant0$，从而 $ab^2c\geqslant0$. 当 $b\neq0$ 时，有 $ac\geqslant0$，即 aRc. 当 $b=0$ 时，取$a=2,c=-3$，则 $ab\geqslant0,bc\geqslant0$. 但 $ac=-6<0$，即 $a\not{R}c$. 故 R 不适合推移律. 所以推移律独立于反射律和对称律.

5. 证明：$[a]=[b]\Rightarrow a\sim b$，其中$[a]=\{x\,|\,x\sim a\}$，$[b]=\{x\,|\,x\sim b\}$.

证 由反射律，$a\sim a$，于是 $a\in[a]$. 因$[a]=[b]$，故 $a\in[b]$，所以 $a\sim b$.

6. 以 1 为代表的模 5 的剩余类，以 1 为代表的模 -5 的剩余类及以 -1 为代表的模 5

的剩余类分别是什么？它们之间有何关系？

解 以 1 为代表的模 5 的剩余类与以 1 为代表的模 -5 的剩余类都是

$$[1]=\left\{q\cdot 5+1\,\middle|\,q\text{ 是整数}\right\}=\left\{q(-5)+1\,\middle|\,q\text{ 是整数}\right\}=\{\cdots,-9,-4,1,6,11,\cdots\},$$

它们相等．而以 -1 为代表的模 5 的剩余类是

$$[-1]=\left\{q\cdot 5+(-1)\,\middle|\,q\text{ 是整数}\right\}=\{\cdots,-11,-6,-1,4,9,\cdots\},$$

它与前两者不相等.

7. 当整数 $n<0$ 时，模 n 的剩余类的全体是下面的哪些情况？

1） $[0],[1],\cdots,[n-1]$.

2） $[0],[1],\cdots,[|n|-1]$.

3） $[0],[-1],\cdots,[n+1]$.

4） $[-1],[-2],\cdots,[n+1],[n+2]$.

5） $[-1],[-2],\cdots,[n+1],[n]$.

解 2)，3)，5).

8. 证明下列所给的各关系～是集 A 的元间的一个等价关系．求出由～决定的 A 的分类及一个全体代表团.

1） A 是所有正整数作成的集.

$$n\sim m\Leftrightarrow n\text{ 与 }m\text{ 的最后一位数字相同.}$$

2） $K=\{1,2,3,4\}$，A 是 K 的全体子集作成的集.

$$S\sim T\Leftrightarrow S\text{ 与 }T\text{ 含有相同个数的元素.}$$

证 1） 关系～所满足的条件可改写为

$$n\sim m\Leftrightarrow 10\,\middle|\,n-m.$$

反射律与对称律显然成立．下面证明推移律．设 $m,n,l\in A$，且 $n\sim m,m\sim l$，则

$$n-m=10q_1,\ m-l=10q_2,\ q_1,q_2\in\mathbb{Z},$$

$$n-l=(n-m)+(m-l)=10(q_1+q_2),$$

从而 $10|n-l$，即 $n\sim l$. 所以推移律成立．于是～是 A 的元间的一个等价关系.

由～决定的含元素 n 的类是

$$[n]=\left\{m\in A\,\middle|\,m\sim n\right\}=\left\{m\in A\,\middle|\,10|m-n\right\}.$$

设

$$m=10q_1+r_1,\ 0\leqslant r_1<10,$$

$$n=10q_2+r_2,\ 0\leqslant r_2<10.$$

则

$$m-n=10(q_1-q_2)+r_1-r_2,\ 0\leqslant|r_1-r_2|<10.$$

其中 r_1 与 r_2 分别是 m 与 n 的最后一位数字．则

$$\begin{aligned}[n]&=\left\{m\in A\,\middle|\,10|10(q_1-q_2)+r_1-r_2\right\}\\&=\left\{m\in A\,\middle|\,10|r_1-r_2\right\}\\&=\left\{m\in A\,\middle|\,r_1=r_2\right\}.\end{aligned}$$

即含 n 的类 $[n]$ 是由与 n 的最后一位数字相同的正整数所组成的．最后一位数字不同的正

整数在不同的类．而最后一位数字共有 10 种选法：1，2，…，9，0. 故得 A 的分类：

$$[1]=\{10q+1 \mid q \text{ 是非负整数}\}=\{1,11,21,\cdots\}.$$

$$[2]=\{10q+2 \mid q \text{ 是非负整数}\}=\{2,12,22,\cdots\}.$$

……………………………………………

$$[9]=\{10q+9 \mid q \text{ 是非负整数}\}=\{9,19,29,\cdots\}.$$

$$[10]=\{10q \mid q \text{ 是正整数}\}=\{10,20,30,\cdots\}.$$

$\{1,2,\cdots,9,10\}$是一个全体代表团.

2）① $\forall S\in A$，S 与 S 含有相同个数的元素，故 $S\sim S$.

② $\forall S,T\in A$，若 $S\sim T$，则 S 与 T 含有相同个数的元素，故 $T\sim S$.

③ $\forall S,T,V\in A$，若 $S\sim T$，$T\sim V$，则 S 与 T 含有相同个数的元素，T 与 V 含有相同个数的元素，故 S 与 V 含有相同个数的元素，即 $S\sim V$.

所以～是 A 的元间的一个等价关系.

由～决定的 A 的分类是：

$$[\varnothing]=\{S\in A \mid S \text{ 与} \varnothing \text{含有相同个数的元素}\}=\{\varnothing\}.$$

$$[\{1\}]=\{S\in A \mid S \text{ 与} \{1\} \text{含有相同个数的元素}\}$$
$$=\{\{1\},\{2\},\{3\},\{4\}\}.$$

$$[\{1,2\}]=\{S\in A \mid S \text{ 与} \{1,2\} \text{含有相同个数的元素}\}$$
$$=\{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}.$$

$$[\{1,2,3\}]=\{S\in A \mid S \text{ 与} \{1,2,3\} \text{含有相同个数的元素}\}$$
$$=\{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}\}.$$

$$[\{1,2,3,4\}]=\{S\in A \mid S \text{ 与} \{1,2,3,4\} \text{含有相同个数的元素}\}$$
$$=\{\{1,2,3,4\}\}=\{K\}.$$

$\{\varnothing,\{1\},\{1,2\},\{1,2,3\},K\}$是一个全体代表团.

9. 设 R 是集 A 的元间的一个关系，证明：

1）R 是 A 的元间的一个等价关系

$\Leftrightarrow$① $\forall a\in A$，aRa；

② $\forall a,b,c\in A$，aRb，$aRc \Rightarrow bRc$.

2）R 是 A 的元间的一个等价关系

$\Leftrightarrow$① 反射律：$\forall a\in A$，aRa；

② 循环律：$\forall a,b,c\in A$，aRb，$bRc \Rightarrow cRa$.

证 1）（$\Rightarrow$）①显然成立．$\forall a,b,c\in A$，aRb，aRc，由对称律，bRa，aRc. 由推移律，bRc. 所以②成立.

（$\Leftarrow$）反射律已成立．$\forall a,b\in A$，aRb，由①，aRa，由②，bRa，所以对称律成立．$\forall a,b,c\in A$，aRb，bRc，由对称律，bRa. 由②，aRc，所以推移律成立．于是 R 是 A 的元间的一个等价关系.

2） （$\Rightarrow$） ①已成立．$\forall a,b,c\in A,aRb,bRc$，由推移律，$aRc$. 由对称律，$cRa$. 所以②成立.

（$\Leftarrow$） 反射律已成立．$\forall a,b\in A,aRb$，由①，bRb，由②，bRa，所以对称律成立．$\forall a,b,c\in A,aRb,bRc$，由②，$cRa$，由对称律 aRc，所以推移律成立．于是 R 是 A 的元间的一个等价关系.

四、思考问题

1. 下面的法则 R 是否为集 A 的元间的一个关系？

1） A 是自然数集，$D=\{$对，错$\}$.

$$R:(n,m)\to \text{对，若 } n+m<0.$$
$$(n,m)\to \text{错，若 } n+m\not<0.$$

2） A 是自然数集，$D=\{$对，错$\}$.

$$R:(n,m)\to \text{对，若 } n+m>0.$$
$$(n,m)\to \text{错，若 } n+m\not>0.$$

3） A 是有理数集，$D=\{$对，错$\}$.

$$R:\left(\frac{b}{a},\frac{d}{c}\right)\to \text{对，若 } b>d.$$
$$\left(\frac{b}{a},\frac{d}{c}\right)\to \text{错，若 } b\not>d.$$

2. 试判断下面的集 A 的子集是否为 A 的一个分类.

1） A 是实数域上的多项式环，$A_0,A_1,A_2,\cdots$ 是 A 的子集，其中 $A_i=\left\{f(x)\in A\,\middle|\,f(x)\text{ 的次数是 } i\right\},i=0,1,2,\cdots$

2） A 是整数集 $\mathbb{Z}$ 的全体变换的集合，A_1,A_2,A_3 是 A 的子集，其中 A_1 是 $\mathbb{Z}$ 的全体单射变换的集合，A_2 是 $\mathbb{Z}$ 的全体满射变换的集合，A_3 是 $\mathbb{Z}$ 的既不是单射又不是满射的变换的集合.

3. 试判断下面的集 A 的元间的关系 R 是否为等价关系.

1） $A=$实数集．

$$xRy\Leftrightarrow y=2x.$$

2） $A=$实数集．

$$xRy\Leftrightarrow x^2+y^2\leqslant 1.$$

3） $A=$实数集．

$$xRy\Leftrightarrow |x-y|\leqslant 1.$$

4） $A=$复数集．

$$z_1Rz_2\Leftrightarrow z_1=z_2+\mathrm{i}.$$

5） $A=$复数集．

$$z_1Rz_2\Leftrightarrow \frac{1}{z_0}(z_1-z_2)\text{ 是实数，其中 } z_0(\neq 0)\text{ 是固定复数．}$$

6） $A=\{a,b\},D=\{$对，错$\}$.

$R(a,a)=R(b,b)=$对，

$R(a,b)=$对，$R(b,a)=$错．

7）　$A=\{a,b,c\}$，$D=\{$对，错$\}$．

$R(a,a)=R(b,b)=R(c,c)=$对，

$R(a,b)=R(b,a)=$对，

$R(a,c)=R(c,a)=$错，

$R(c,b)=R(b,c)=$对．

4. 设 $a\equiv b(n)$，$c\equiv d(n)$，证明：

1）　$a\pm c\equiv b\pm d(n)$．

2）　$ma\equiv mb(n)$，其中 m 是任一整数．

3）　$ac\equiv bd(n)$．

5. 求出由下列各等价关系～决定的集 A 的分类．

1）　A 是复数集．

$$a+b\mathrm{i}\sim c+d\mathrm{i}\Leftrightarrow a^2+b^2=c^2+d^2.$$

2）　A 是实数集．

$$x\sim y\Leftrightarrow x^2=y^2.$$

3）　A 是实数域上一切 n 阶矩阵所作成的集合．

$$X\sim Y\Leftrightarrow \exists\text{可逆矩阵 }P\in A\text{，使得 }PX=Y.$$

4）　A 是实数域 $\mathbb{R}$ 上一切 n 阶矩阵所作成的集合．

$$X\sim Y\Leftrightarrow |X|=|Y|.$$

5）　A 是实数域上一切 n 阶矩阵所作成的集合．

$$X\sim Y\Leftrightarrow \exists\text{可逆矩阵 }P\in A\text{，使得 }X=P^{-1}YP.$$

6）　A 是实数域上一切 n 阶矩阵所作成的集合．

$$X\sim Y\Leftrightarrow \text{秩 }X=\text{秩 }Y.$$

7）　$A=\{(x,y)\mid x,y\text{ 都是实数，}x\neq 0\text{ 且 }y\neq 0\}$．

$$(x_1,y_1)\sim(x_2,y_2)\Leftrightarrow x_1x_2>0\text{ 且 }y_1y_2>0.$$

8）　A 是实数集，$[x]$表示小于或等于实数 x 的最大整数．

$$x\sim y\Leftrightarrow [x]=[y].$$

第四章　群的定义、有限群的另一定义

一、基本问题问答

1. 群的定义比较常见的有两种.

群的第一定义　我们说，一个不空集合 G 对于一个叫做乘法的代数运算来说作成一个群，假如

Ⅰ. G 对于这个乘法来说是封闭的；

Ⅱ. 结合律成立：

$$a(bc)=(ab)c$$

对于 G 的任意三个元 a,b,c 都对；

Ⅲ. 对于 G 的任意两个元 a,b 来说，方程

$$ax=b \quad 和 \quad ya=b$$

都在 G 里有解.

群的第二定义　我们说，一个不空集合 G 对于一个叫做乘法的代数运算来说作成一个群，假如

Ⅰ. G 对于乘法来说是封闭的；

Ⅱ. 结合律成立：

$$a(bc)=(ab)c$$

对于 G 的任意三个元 a,b,c 都对；

Ⅳ. G 里至少存在一个左单位元 e，能让

$$ea=a$$

对于 G 的任何元 a 都成立；

Ⅴ. 对于 G 的每一个元 a，在 G 里至少存在一个左逆元 a^{-1}，能让

$$a^{-1}a=e.$$

把群的第二定义中的Ⅳ改为"$\forall a\in G,\exists e\in G$，使得 $ea=a$"，是否可以？

答　不可．因为这里 e 随 a 的变化而变化，而Ⅳ"$\exists e\in G$，使得 $\forall a\in G, ea=a$"中的 e 不因 a 的变化而变化.

注　同样应注意Ⅴ不可改为"$\exists b\in G$，使得 $\forall a\in G$ 有 $ba=e$"，因为这里 b 不因 a 的变化而变化，而Ⅴ中的 a^{-1} 随 a 的变化而变化.

2. 对Ⅳ作如下证明："$\forall a\in G$，由Ⅲ，方程 $ya=a$ 在 G 里有解，从而 $\exists e\in G$，使得 $ea=a$"，是否可以？

答　不可．因为这里 e 随 a 的变化而变化，不符合Ⅳ的要求.

3. 设 $a,b\in$ 群 G，如何判断元 b 是元 a 的逆元？证明：$(a^{-1})^n=(a^n)^{-1}$，其中 n 是整数.

答　$b=a^{-1} \Leftrightarrow ab=e$，$e$ 是 G 的单位元

$\Leftrightarrow ba=e$，e 是 G 的单位元.

因 $a^n(a^{-1})^n=a^na^{-n}=a^{n+(-n)}=a^0=e$，故 $(a^n)^{-1}=(a^{-1})^n$.

4. 群 G 的元 a 的阶的定义是什么？

答　a 的阶是正整数 n，即 $|a|=n$

$\Leftrightarrow$ 1)　n 是正整数，使得 $a^n=e$；

2)　$\forall$ 正整数 k，$k<n$，都使得 $a^k\neq e$.

$\Leftrightarrow$ 1)　n 是正整数，使得 $a^n=e$；

2)　若 $a^k=e$，k 是正整数，则 $k\geqslant n$.

a 的阶无限，即 $|a|=\infty$

$\Leftrightarrow$ $\forall$ 正整数 m，都使 $a^m\neq e$.

$\Leftrightarrow$ 若 $a^n=e$，则 $n=0$.

a 的阶有限

$\Leftrightarrow$ a 的阶是一个正整数

$\Leftrightarrow$ $\exists$ 正整数 n，使得 $a^n=e$.

注　a 是群 G 的单位元 $\Leftrightarrow$ $|a|=1$.

5. 证明：设 $a\in$ 群 G，若有正整数 n，使得 $a^n=e$，则 $|a|\leqslant n$.

证　作集 $A=\{k\,|\,k$ 是正整数，$a^k=e\}$，由已知，$n\in A$，从而 $A\neq\varnothing$. 由最小数原理，A 有最小数 m，使得 $a^m=e$. 所以 $|a|=m\leqslant n$.

例　e 是群 G 的单位元，有 $e^3=e$，但 $|e|\neq 3$，而 $|e|=1$.

6. 证明：设 $a\in$ 群 G，且 $|a|=n$，则

$$a^m=e\Leftrightarrow n\mid m.$$

证　($\Rightarrow$)　设 $m=qn+r$，$0\leqslant r<n$，则

$$r=m-qn,$$

从而

$$a^r=a^{m-qn}=a^m\cdot a^{-qn}=e\cdot(a^n)^{-q}=e\cdot e^{-q}=e.$$

因 $|a|=n$，又 $0\leqslant r<n$，故 $r=0$，所以 $n|m$.

($\Leftarrow$)　$n|m$

$\Rightarrow m=qn$

$\Rightarrow a^m=a^{qn}=(a^n)^q=e^q=e.$

例　若 $a\in$ 群 G，p 是素数，使得 $a^p=e$，则 $|a|$ 可能是 p，也可能不是 p 而是 1.

注　命题“设 $a\in$ 群 G，且 $a^m=e$，若 $n|m$，则 $|a|=n$”不成立.

例　非零有理数集 $\mathbf{Q}^*$ 对于普通乘法来说作成一个群，1 是 $\mathbf{Q}^*$ 的单位元，取 $-1\in\mathbf{Q}^*$，$(-1)^8=1$. 又 $4|8$，但 $|-1|\neq 4$，而是 $|-1|=2$.

7. 设 $a\in$ 群 G，且 $|a|=m$，m 是正整数，证明：

$$a^0=e,a,a^2,\cdots,a^{m-1}$$

是 G 中 m 个不同的元.

证　（反证法）

若 $a^i=a^j,0\leqslant i<j\leqslant m-1$

$\Rightarrow a^i\cdot a^{-i}=a^j\cdot a^{-i}$

$\Rightarrow a^{j-i}=a^0=e$，但 $0<j-i\leqslant m-1$，

从而 $|a|\leqslant j-i\leqslant m-1$. 此与 $|a|=m$ 矛盾. 所以

$$a^0=e,a,a^2,\cdots,a^{m-1}$$

是 G 中 m 个不同的元.

8. 设 $a\in$群 G，证明：

$$|a|=\infty\Leftrightarrow \text{下面无穷多个元}$$
$$\cdots,a^{-2},a^{-1},a^0=e,a,a^2,\cdots$$

互不相同.

证 $(\Rightarrow)$ (反证法)若 $a^i=a^j,i<j$，则 $a^{j-i}=e$，其中 $j-i>0$，从而 a 的阶有限，此与假设矛盾.

$(\Leftarrow)$ (反证法)若 a 的阶有限，则必有正整数 m，使得 $a^m=e=a^0$，此与已知

$$\cdots,a^{-2},a^{-1},a^0=e,a,a^2,\cdots$$

互不相同矛盾.

注 若群 G 中有一个元 a 的阶无限，则 G 必为无限群.

9. 设有限集 $G=\{a_1,a_2,\cdots,a_n\}$，其代数运算是如下乘法表

	a_1	a_2	$\cdots$	a_n
a_1	a_{11}	a_{12}	$\cdots$	a_{1n}
a_2	a_{12}	a_{22}	$\cdots$	a_{2n}
$\vdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
a_n	a_{n1}	a_{n2}	$\cdots$	a_{nn}

证明：

G 的乘法适合消去律 $\Leftrightarrow$ 在 G 的乘法表中，每一行(列)中的 n 个元素互不相同.

证 $(\Rightarrow)$ 不然，若在第 i 行元素中有 $a_{ih}=a_{ik},h\neq k$，即 $a_ia_h=a_ia_k$. 因 G 的乘法适合消去律，故 $a_h=a_k$，产生矛盾. 所以每一行中的元素互不相同.

同理，每一列中的元素也互不相同.

$(\Leftarrow)$ 不然，若消去律不成立，必有 $a_ia_s=a_ia_t$，但 $a_s\neq a_t$. 由 $a_ia_s=a_ia_t$，得 $a_{is}=a_{it}$. 由 $a_s\neq a_t$，得 $s\neq t$，即 a_{is} 与 a_{it} 在不同列，于是 G 的乘法表中第 i 行出现相同元素. 此与已知矛盾. 所以 G 的乘法适合消去律.

二、典型问题分析

1. 全体整数的集合对于普通减法来说是不是一个群?

解一 因为

$$(4-2)-1\neq 4-(2-1).$$

即减法结合律不成立．所以整数集对于普通减法来说不是一个群.

解二　因为当 $c\neq 0$ 时，

$$(a-b)-c\neq a-(b-c).$$

即减法结合律不成立．所以整数集对于普通减法来说不是一个群.

注　$(a-b)-c\neq a-(b-c)$，应注明条件当 $c\neq 0$ 时.

2. 举一个有两个元的群的例子.

解一　$G=\{1,-1\}$对普通乘法来说是一个群．事实上，$G\neq\varnothing$.

Ⅰ．因 $1\times1=1$，$1\times(-1)=-1$，$(-1)\times1=-1$，$(-1)\cdot(-1)=1$ 都 $\in G$，故 G 对乘法封闭；

Ⅱ．数的乘法结合律成立；

Ⅳ．1 是 G 的单位元；

Ⅴ．1 的逆元是 1，-1 的逆元是 -1.

解二　$G=\{a,b\}$对于代数运算

	a	b
a	a	b
b	b	a

来说是一个群．事实上，$G\neq\varnothing$.

Ⅰ．因 $aa=a$，$ab=b$，$ba=b$，$bb=a$ 都$\in G$，故 G 对乘法封闭；

Ⅱ．因

$$(aa)a=a(aa),\quad (aa)b=a(ab),$$
$$(ab)a=a(ba),\quad (ab)b=a(bb),$$
$$(ba)a=b(aa),\quad (ba)b=b(ab),$$
$$(bb)a=b(ba),\quad (bb)b=b(bb).$$

故结合律成立；

Ⅳ．a 是 G 的单位元；

Ⅴ．a 的逆元是 a，b 的逆元是 b.

注　利用群的第二定义验证较第一定义简便，因为利用第一定义需分别验证 8 个方程.

$$ax=a,\quad ax=b,$$
$$bx=a,\quad bx=b,$$
$$ya=a,\quad ya=b,$$
$$yb=a,\quad yb=b$$

都在 G 中有解.

3. 证明：我们也可以用条件Ⅰ，Ⅱ以及下面的条件Ⅳ$'$，Ⅴ$'$来作群的定义.

Ⅳ$'$．G 里至少存在一个右单位元 e，能让

$$ae=a$$

对于 G 的任何元 a 都成立.

Ⅴ′. 对于 G 的每一个元 a，在 G 里至少存在一个右逆元 a^{-1}，能让

$$a a^{-1} = e.$$

证一 下面证明，设 $G\neq\varnothing$，则

$$\text{Ⅰ},\text{Ⅱ},\text{Ⅲ} \Leftrightarrow \text{Ⅰ},\text{Ⅱ},\text{Ⅳ}',\text{Ⅴ}'$$

($\Rightarrow$) Ⅰ，Ⅱ已成立. 今证Ⅳ′

取定 $b\in G$，由Ⅲ，方程 $bx=b$ 在 G 里有解，即 $\exists e\in G$，使得

$$be=b.$$

（这里 e 随 b 的变化而变化.）要证Ⅳ′，需证明：$\exists e\in G$，使得 $\forall a\in G, ae=a$，这里 e 不因 a 的变化而变化. 为此，$\forall a\in G$，由Ⅲ，方程 $yb=a$ 有解 c，且 $c\in G$，即

$$cb=a,$$

从而

$$ae=(cb)e=c(be)=cb=a.$$

所以Ⅳ′成立.

再证Ⅴ′. $\forall a\in G$，由Ⅲ，方程 $ax=e$ 在 G 里有解，从而 $\exists a^{-1}\in G$，使得

$$a a^{-1} = e,$$

其中 e 是右单位元. 所以Ⅴ′成立.

($\Leftarrow$) Ⅰ，Ⅱ已成立. 今证Ⅲ.

1) 一个右逆元 a^{-1} 一定也是一个左逆元. 即由

$$a a^{-1} = e,$$

其中 e 是右单位元. 可以证明

$$a^{-1}a = e.$$

因为由Ⅴ′，对于 $a^{-1}\in G$ 来说，$\exists$ a^{-1} 的右逆元 $a'\in G$，使得

$$a^{-1} a' = e,$$

其中 e 是右单位元. 所以

$$a^{-1}a = (a^{-1} a)e = (a^{-1} a)(a^{-1} a') = (a^{-1}(a a^{-1}))a' = (a^{-1} e)a' = a^{-1}a' = e.$$

于是右逆元 a^{-1} 也是左逆元.

2) 一个右单位元 e 一定也是一个左单位元. 即 $\forall a\in G$，由

$$ae=a,$$

可以证明

$$ea=a.$$

事实上，

$$ea=(a a^{-1})a=a(a^{-1} a)\overset{\text{由 1)}}{=\!=\!=} ae=a.$$

于是右单位元 e 也是左单位元.

3) $\forall a,b\in G$，方程

$$ax = b$$

在 G 里有解. 事实上，由Ⅴ′，Ⅰ，$\exists$ $a^{-1}b\in G$，使得

$$a(a^{-1}b)=(a a^{-1})b=eb\overset{\text{由 2)}}{=\!=\!=} b.$$

同样，$\forall a,b\in G$，方程

$$ya=b$$

在 G 里有解．事实上，由 Ⅴ$'$，Ⅰ，$\exists\ ba^{-1}\in G$，使得

$$(ba^{-1})a=b(a^{-1}a)\overset{\text{由}1)}{=\!=}be\overset{\text{Ⅳ}'}{=\!=}b.$$

所以Ⅲ成立.

证二　下面证明，设 $G\neq\varnothing$，则

$$\text{Ⅰ},\text{Ⅱ},\text{Ⅳ},\text{Ⅴ}\Leftrightarrow\text{Ⅰ},\text{Ⅱ},\text{Ⅳ}',\text{Ⅴ}'.$$

($\Leftarrow$)　Ⅰ，Ⅱ已成立．今证Ⅳ.

由Ⅳ$'$，$\exists$ 右单位元 $e\in G$，使得 $\forall a\in G$，$ae=a$．由证一($\Leftarrow$)2)，右单位元 e 也是左单位元，因此，$\exists$ 左单位元 e，使得 $\forall a\in G$，$ea=a$，即Ⅳ成立.

再证Ⅴ．由Ⅴ$'$，$\forall a\in G$，$\exists$ 右逆元 $a^{-1}\in G$，使得 $aa^{-1}=e$，其中 e 是 G 的右单位元．由证一($\Leftarrow$)1)，右逆元 a^{-1} 也是左逆元，从而 $\forall a\in G$，$\exists$ 左逆元 $a^{-1}\in G$，使得 $a^{-1}a=e$，其中 e 是 G 的右单位元．再由证一($\Leftarrow$)2)，右单位元也是左单位元，因此，$\forall a\in G$，$\exists$ 左逆元 $a^{-1}\in G$，使得 $a^{-1}a=e$，其中 e 是 G 的左单位元．即Ⅴ成立.

($\Rightarrow$)　略.

证三　下面证明，设 $G\neq\varnothing$，则

$$\text{Ⅰ},\text{Ⅱ},\text{Ⅳ},\text{Ⅴ}\Leftrightarrow\text{Ⅰ},\text{Ⅱ},\text{Ⅳ}',\text{Ⅴ}'.$$

($\Leftarrow$)　Ⅰ，Ⅱ已成立.

由Ⅳ$'$，$\exists$ 右单位元 $e\in G$，使得 $\forall a\in G$，$ae=a$．由Ⅴ$'$，$\forall a\in G$，$\exists$ 右逆元 $a^{-1}\in G$，使得 $aa^{-1}=e$，其中 e 是 G 的右单位元．对于 $a^{-1}\in G$，由Ⅴ$'$，$\exists\ a^{-1}$ 的右逆元 $a'\in G$，使得 $a^{-1}a'=e$，其中 e 是 G 的右单位元．于是

$$ea'=(aa^{-1})a'=a(a^{-1}a')=ae=a.$$

今证Ⅳ：$\exists$ 右单位元 $e\in G$，使得 $\forall a\in G$，

$$ea=e(ea')=(ee)a'=ea'=a,$$

从而右单位元 e 也是左单位元，所以Ⅳ成立.

再证Ⅴ：$\forall a\in G$，$\exists$ 右逆元 $a^{-1}\in G$，使得

$$a^{-1}a=a^{-1}(ea')=(a^{-1}e)a'=a^{-1}a'=e,$$

从而右逆元 a^{-1} 也是左逆元，所以Ⅴ成立.

($\Rightarrow$)　同理可证.

证四　下面证明，设 $G\neq\varnothing$，则

$$\text{Ⅰ},\text{Ⅱ},\text{Ⅳ},\text{Ⅴ}\Leftrightarrow\text{Ⅰ},\text{Ⅱ},\text{Ⅳ}',\text{Ⅴ}'.$$

($\Leftarrow$)　Ⅰ，Ⅱ已成立．今证Ⅳ.

由Ⅳ$'$，$\exists$ 右单位元 $e\in G$，使得 $\forall a\in G$，$ae=a$．只需证右单位元 e 也是左单位元．$\forall a\in G$，设

$$ea=b$$

$$\overset{\mathrm{V}'}{\Rightarrow}\ (ea)a^{-1}=b\,a^{-1}\text{，其中 }a^{-1}\text{ 是 }a\text{ 的右逆元}$$
$$\overset{\mathrm{II}}{\Rightarrow}\ e(a\,a^{-1})=b\,a^{-1}$$
$$\overset{\mathrm{V}'}{\Rightarrow}\ ee=b\,a^{-1}$$
$$\overset{\mathrm{IV}'}{\Rightarrow}\ e=b\,a^{-1}$$
$$\overset{\mathrm{V}'}{\Rightarrow}\ a\,a^{-1}=b\,a^{-1},$$

其中 a^{-1}是 a 的右逆元．对于 $a^{-1}\in G$,由Ⅴ′,∃ a^{-1}的右逆元 $a'\in G$,使得 $a^{-1}a'=e$,其中 e 是右单位元,所以

$$\begin{aligned}&a\,a^{-1}=b\,a^{-1}\\ \Rightarrow\ &(a\,a^{-1})a'=(b\,a^{-1})a'\\ \Rightarrow\ &a(a^{-1}a')=b(a^{-1}a')\\ \Rightarrow\ &ae=be\\ \Rightarrow\ &a=b\\ \Rightarrow\ &ea=a.\end{aligned}$$

因此,右单位元 e 也是左单位元,从而Ⅳ成立.

再证Ⅴ．由Ⅴ′,$\forall a\in G$,∃右逆元 $a^{-1}\in G$,使得$a\,a^{-1}=e$,其中 e 是右单位元．只需证右逆元 a^{-1}也是左逆元．设

$$\begin{aligned}&a^{-1}a=c\\ \Rightarrow\ &(a^{-1}a)a^{-1}=c\,a^{-1}\\ \Rightarrow\ &a^{-1}(a\,a^{-1})=c\,a^{-1}\\ \Rightarrow\ &a^{-1}e=c\,a^{-1}\text{，其中 }e\text{ 是右单位元也是左单位元}\\ \Rightarrow\ &e\,a^{-1}=c\,a^{-1}.\end{aligned}$$

对于 $a^{-1}\in G$,由Ⅴ′,∃ a^{-1}的右逆元 $a'\in G$,使得 $a^{-1}a'=e$,其中 e 是右单位元,所以

$$\begin{aligned}&ea^{-1}=ca^{-1}\\ \Rightarrow\ &(ea^{-1})a'=(ca^{-1})a'\\ \Rightarrow\ &e(a^{-1}a')=c\,(a^{-1}a')\\ \Rightarrow\ &ee=ce\\ \Rightarrow\ &e=c\\ \Rightarrow\ &a^{-1}a=e.\end{aligned}$$

因此,右逆元 a^{-1}也是左逆元,从而Ⅴ成立.

(⇒)　同理可证.

证五　下面证明,设 $G\neq\varnothing$,则

$$\mathrm{I},\mathrm{II},\mathrm{III}\Leftrightarrow \mathrm{I},\mathrm{II},\mathrm{IV}',\mathrm{V}'.$$

(⇐)　Ⅰ,Ⅱ已成立.

由Ⅳ′,∃右单位元 $e\in G$,使得 $\forall a\in G,ae=a$. 由Ⅴ′,$\forall a\in G$,∃右逆元 $a^{-1}\in G$,使得 $a\,a^{-1}=e$,其中 e 是 G 的右单位元．对于 $a^{-1}\in G$,由Ⅴ′,∃ a^{-1}的右逆元 $a'\in G$,使得 $a^{-1}a'=e$,其中 e 是 G 的右单位元．于是

$$ea'=(a\,a^{-1})a'=a(a^{-1}a')=ae=a.$$

对于 $b^{-1}\in G$，同理有 b^{-1} 的右逆元 $b'\in G$，使得 $eb'=b$. 今证 $\forall a,b\in G$，方程 $ax=b$ 在 G 里有解．事实上，由 Ⅴ′，Ⅰ，$\exists\ a^{-1}b\in G$，使得

$$a(a^{-1}b)=(aa^{-1})b=eb=e(eb')=(ee)b'=eb'=b.$$

同样，$\forall a,b\in G$，方程 $ya=b$ 在 G 里有解．事实上，由 Ⅴ′，Ⅰ，$\exists\ ba^{-1}\in G$，使得

$$\begin{aligned}(ba^{-1})a &=(ba^{-1})(ea')=\big((ba^{-1})e\big)a'=(ba^{-1})a'=b(a^{-1}a')\\ &=be=b.\end{aligned}$$

（$\Rightarrow$）　见证一.

4. 证明：若群 G 的每一个元都适合方程 $x^2=e$，那么 G 是交换群.

证一　$\forall a,b\in G$，

$$\begin{aligned}&a^2b^2=e,\quad (ab)^2=e\\ &\Rightarrow aabb=abab\\ &\xrightarrow{\text{消去律}} ab=ba.\end{aligned}$$

证二　$\forall a,b\in G$，

$$\begin{aligned}&(ab)(ba)=ab^2a=aea=a^2=e,\\ &(ab)(ab)=(ab)^2=e\\ &\Rightarrow (ab)(ba)=(ab)(ab)\\ &\xrightarrow{\text{消去律}} ba=ab.\end{aligned}$$

证三　$\forall a,b\in G$，

$$\begin{aligned}ba&=(ba)e=(ba)(ab)^2=baab(ab)\\ &=ba^2b(ab)=beb(ab)=b^2(ab)=e(ab)\\ &=ab.\end{aligned}$$

证四　$\forall a\in G$，

$$\begin{aligned}&a^2=e\\ &\Rightarrow a^{-1}=a.\end{aligned}$$

$\forall a,b\in G$，

$$ab=(ab)^{-1}=b^{-1}a^{-1}=ba.$$

注　1）　G 是群，$\forall a\in G$，则

$$\begin{aligned}&a^2=e\\ &\Leftrightarrow a\text{ 的阶}\leqslant 2\\ &\Leftrightarrow a^{-1}=a\\ &\Rightarrow G\text{ 是交换群}.\end{aligned}$$

2）　该命题的逆命题不成立.

例　整数加群 $\mathbb{Z}$ 是交换群，$3\in\mathbb{Z}$，但 $2\cdot 3\neq 0$，即 3 的阶$\not\leqslant 2$，实际上，3 的阶$=\infty$.

3）　若 $a,b\in$群 G，且 a,b 与 ab 都是 2 阶元，则 a 与 b 可交换.

5. 证明：在一个有限群里阶大于 2 的元的个数一定是偶数.

证　题中"阶大于 2 的元"指阶为有限的元，即阶是正整数的元．因此只需证明阶大于 2 的元是成双出现的.

1）　若 $|a|$ 是 n，则 $|a^{-1}|$ 也是 n.

事实上，因 $a^n=e$，故

$$(a^{-1})^n=(a^n)^{-1}=e^{-1}=e.$$

又若有正整数 $m<n$，使 $(a^{-1})^m=e$

$$\Rightarrow a^m=((a^{-1})^{-1})^m=((a^{-1})^m)^{-1}=e^{-1}=e$$

$$\Rightarrow |a|\leqslant m<n.$$

此与 $|a|=n$ 矛盾．所以 $|a^{-1}|=n$.

2） 若 $|a|>2$，则 $a\neq a^{-1}$.

不然，若 $a=a^{-1}$，则 $aa=a\,a^{-1}$，即 $a^2=e$，从而 $|a|\leqslant 2$. 此与 $|a|>2$ 矛盾.

3） 若 $b\neq a$，则 $b^{-1}\neq a^{-1}$.

不然，若 $a^{-1}=b^{-1}$，则 $(a^{-1})^{-1}=(b^{-1})^{-1}$，即 $a=b$. 此与假设矛盾.

4） 若 $b\neq a^{-1}$，则 $b^{-1}\neq a$.

不然，若 $b^{-1}=a$，则 $(b^{-1})^{-1}=a^{-1}$，即 $b=a^{-1}$．此与假设矛盾.

综上，阶大于 2 的元 a 与 a^{-1} 成双出现．又有限群里元的个数是一个有限正整数．所以有限群里阶大于 2 的元的个数一定是偶数.

注 还可如下证明 $|a|=|a^{-1}|$.

设 $|a|=n$，$|a^{-1}|=m$，只需证 $n|m$，$m|n$.

由 $a^n=e$，有 $(a^{-1})^n=e$，因此 $m|n$. 因 a 与 a^{-1} 互为逆元，故 $n|m$，又 n,m 都是正整数，从而 $n=m$，即 $|a|=|a^{-1}|$.

若 $|a|=\infty$，则 $|a^{-1}|=\infty$. 不然，假设 $|a^{-1}|=k$，k 是正整数，则同理可证 $|a|=k$. 此与 $|a|=\infty$ 矛盾.

6. 证明：一个有限群的每一个元的阶都有限.

证一 设 G 是有限群，$\forall a\in G$，由 G 对乘法封闭，有

$$a,a^2,\cdots,a^m,\cdots,a^n,\cdots \text{ 都 } \in G.$$

因 G 是有限群，故必有 a^m，$a^n(m<n)$，

$$a^n=a^m$$

$$\Rightarrow a^n a^{-m}=a^m a^{-m}$$

$$\Rightarrow a^{n-m}=a^0=e,$$

其中 $n-m$ 是一个正整数，从而 $|a|\leqslant n-m$. 所以 G 的每个元的阶都有限.

证二 （反证法）若 G 是有限群．假设有某 $a\in G$，$|a|$ 无限，则由 G 对乘法封闭，有

$$a^0,a,a^2,\cdots,a^n,\cdots \text{ 都 } \in G,$$

且它们互不相同．不然，若有 $a^h=a^k$，$h>k$，

$$a^{h-k}=a^h a^{-k}=a^k a^{-k}=a^{k-k}=a^0=e,$$

其中 $h-k$ 是一个正整数，从而 $|a|$ 有限．此与假设矛盾．所以，G 中有无穷多个元．此与 G 是有限群矛盾．于是 $\forall a\in G$，$|a|$ 有限.

注 1） 该命题的逆命题："每一个元的阶都有限的群是有限群"不成立.

例

$G=\left\{z\,\middle|\,z \text{ 是复数}, z^n=1, n=1,2,\cdots\right\}$ 对于普通乘法来说作成一个群.

事实上，我们已知非零复数集 $\mathbb{C}^*$ 对于复数乘法封闭．$\forall x,y\in G$，$\exists$ 自然数 m,n，使得 $x^m=1$，$y^n=1$. 令 k 是 m,n 的最小公倍数，则 $(xy)^k=x^ky^k=1$，从而 $xy\in G$，所以 G 对于复

数乘法封闭．又 $\forall x\in G$，$\exists$ 自然数 n，使得 $x^n=1$，则 $(x^{-1})^n=(x^n)^{-1}=1$，从而 $x^{-1}\in G$. 因此，G 是 $\mathbb{C}^*$ 的一个子群.

$\forall z\in G$，$\exists$ 正整数 m，使得 $z^m=1$. 故 G 中每个元的阶都有限，但 G 是无限群.

后面第八章，四，2，3）与第十七章，三，1，8）又给出了无限群的每个元的阶都有限的例子.

2）　若群 G 中有一个元的阶是无限的，那么 G 必为无限群.

3）　无限群中除单位元是 1 阶元外，可能所有元都是有限阶的，如注 1）中例；也可能除单位元以外所有元都是无限阶的，如整数加群；还可能有些元是无限阶的，而有些元却是有限阶的，如全体非零有理数对普通乘法作成的群，元 3 的阶是无限，而元 -1 的阶是 2.

7. 证明：假定 G 是一个阶是偶数的有限群．在 G 里阶等于 2 的元的个数一定是奇数.

证　由上题．有限群 G 的每一个元的阶都有限，因此，G 的阶 $|G|=$ 阶大于 2 的元的个数 + 阶等于 2 的元的个数 + 阶小于 2 的元的个数．令 $|G|$ 为偶数 $2n$. 又由上面 5 题，有限群 G 里阶大于 2 的元的个数是偶数 $2m$，而阶小于 2(即阶等于 1)的元只能是单位元，因此只有 1 个，从而 G 里阶等于 2 的元的个数 $=2n-(2m+1)=2(n-m)-1$ 是一个奇数.

注　由此题知，任意偶数阶有限群至少有一个二阶元.

三、讲与练

1. 取定自然数 n，证明：

$$U_n=\left\{z\,\middle|\,z\text{ 是复数},z^n=1\right\}$$

对于复数乘法作成群，称 U_n 为 n 次单位根乘群.

证　Ⅰ. $\forall z_1,z_2\in U_n$，则 $z_1^n=1,z_2^n=1$. 于是 $(z_1z_2)^n=z_1^n z_2^n=1$，从而 $z_1 z_2\in U_n$，即 U_n 对于乘法封闭.

Ⅱ. 数的乘法结合律成立.

Ⅳ. $1(\in U_n)$ 是 U_n 的单位元.

Ⅴ. $\forall z\in U_n$，$(z^{-1})^n=\left(\frac{1}{z}\right)^n=\frac{1}{z^n}=1$，从而 $\exists z^{-1}\in U_n$，使得 $z^{-1}z=1$.

所以，U_n 是一个群.

2. 判断以下各命题是否正确.

1）　设 $\mathbb{N}$ 是全体自然数作成的集合，$\mathbb{N}$ 的代数运算是数的加法，则数零是 $\mathbb{N}$ 的左单位元和右单位元.

2）　设 S 是不空集合，S 的代数运算是

$$ab=b.$$

则 S 中任一元都是 S 的左单位元，但 S 没有右单位元.

3）　设 G 是有代数运算的非空集合，存在单位元 e，并且每一元都有逆元，则 G 是一个群.

4）　设 G 是有代数运算的非空集合，结合律成立，且在 G 中至少存在一个左单位元，又对于每一元 $a\in G$，存在一个左单位元 $e\in G$ 以及 $b\in G$，使得 $ba=e$，则 G 是一个群.

5）　设 G 是有代数运算的非空集合，结合律成立，$\exists$ 左单位元 $e\in G$，并且 $\forall a\in G$，$\exists a$

的右逆元$b\in G$,使得$ab=e$,则G是一个群.

6) 设G是有代数运算的非空集合,且结合律成立,$\forall a,b\in G$,$ax=b$在G中有解,则G是一个群.

7) 设G是有代数运算的非空集合,结合律成立,且$\forall a,b\in G$,$ax=b$在G中有且只有一个解,则G是一个群.

8) 设G是有代数运算的非空集合,结合律成立,且$\forall a,b\in G$,$ax=b$在G中有解,$ya=a$在G中有解,则G是一个群.

解 1) 不正确. 因为数零不是$\mathbb{N}$中的元素. 事实上,$\mathbb{N}$既无左单位元又无右单位元.

(这种没有左单位元和右单位元的集合是很多的. 例如,$G_1=\{f(x)\mid f(x)$是复数域上的多项式,次$(f(x))>0\}$,代数运算是多项式乘法. 又例如,$G_2=\{(a,b)\mid a,b$是实数$\}$,代数运算是:$(a,b)(c,d)=(0,0)$. 再例如,$\mathbb{Z}$是整数集,代数运算是:$nm=\max(n,m)$,等等.)

2) 不正确. S中任一元都是S的左单位元. 当S只含一个元素时,S有右单位元. 但当S含有多于1个的元素时,S就没有右单位元. 不然,若S有右单位元e,则取$a\in A$,$a\neq e$,有$ae=a$,但按规定的代数运算,$ae=e$,从而$a=e$,发生矛盾.

3) 不正确.

例 设$G=\{e,a,b\}$,乘法表为

	e	a	b
e	e	a	b
a	a	e	a
b	b	b	e

G有单位元e,且e,a,b的逆元分别是e,a,b,但因

$$(aa)b=eb=b,\quad a(ab)=aa=e.$$

故

$$(aa)b\neq a(ab),$$

从而结合律不成立. 所以G不是一个群.

(不能找到仅含有两个元,适合上述条件而不是群的例子. 设$G=\{e,a\}$,G有单位元e,使得$ea=ae=a$,且$ee=e$,即e的逆元是e. 因G中每一元都有逆元,故a的逆元只能是a,即$aa=e$. 这样,G是一个群.)

下面我们再举出一个例子.

设G是全体非负实数集,代数运算是:

$$a\cdot b=|a-b|.$$

则$\exists 0\in G$,使得$\forall a\in G$,$0\cdot a=|0-a|=a$,从而G有单位元0. $\forall a\in G$,$\exists a\in G$,使得$a\cdot a=|a-a|=0$,从而G中每个元a都以自身为其逆元. 但

$$(1\cdot 2)\cdot 3=|1-2|\cdot 3=|1-3|=2,$$
$$1\cdot(2\cdot 3)=1\cdot|2-3|=|1-1|=0,$$

从而

$$(1\cdot 2)\cdot 3\neq 1\cdot(2\cdot 3).$$

即结合律不成立．所以 G 不是一个群.

4）　不正确.

例　设 G 是一个至少含两个元的集合．代数运算是

$$xy=y.$$

$\forall x,y,z\in G$，

$$(xy)z=yz=z,\quad x(yz)=xz=z.$$

所以结合律成立．G 中每个元都是左单位元．$\forall x\in G$，$\exists$ 左单位元 $x\in G$ 以及 $y\in G$，使得 $yx=x$，因此 G 满足全部已知条件．但 $\forall x\in G$，对于左单位元 $e(\neq x)$ 来说，$\bar{\exists}\, y\in G$，使得 $yx=e$，即 x 无左逆元，从而Ⅳ不成立（或：$\forall u,v\in G$，当 $u\neq v$ 时，方程 $yu=v$ 在 G 中无解，从而Ⅲ不成立）．所以 G 不是一个群.

5）～8）都不正确．4）中的例子适合 5）～8）的全部已知条件，但 G 不是一个群．我们还可以举出许多这样的例子，下面我们举出一些说明 5）不正确的例子.

例 1　设 $G=\{e,a\}$．乘法表如下：

	e	a
e	e	a
a	e	a

因

$$(ee)e=e(ee),\quad (ee)a=e(ea),$$
$$(ea)e=e(ae),\quad (ea)a=e(aa),$$
$$(ae)e=a(ee),\quad (ae)a=a(ea),$$
$$(aa)e=a(ae),\quad (aa)a=a(aa).$$

故结合律成立．$\exists e\in G$，使得 $\forall x\in G$，有 $ex=x$，从而 e 是 G 的左单位元．$\forall x\in G$，$\exists e\in G$，使得 $xe=e$，从而 x 有右逆元 e．所以 G 满足题设条件，但 G 不是一个群．事实上，e 是 G 的左单位元，但 $a\in G$，而 $\forall x\in G$，$xa=a\neq e$，从而 a 无左逆元.

例 2　设 $G=\{e,a,b\}$．乘法表如下：

	e	a	b
e	e	a	b
a	e	a	b
b	e	a	b

因为两个元素的积就是后者，所以

$$(xy)z=z=x(yz).$$

故结合律成立．e 既为 G 的左单位元，又为每个元的右逆元．于是 G 满足题设条件，但 G 不是一个群，因为 G 没有单位元.

例 3　设 $G=\{e_1,e_2,a,b\}$，其中

$$e_1=\begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix},\ e_2=\begin{pmatrix}1 & -1\\ 0 & 0\end{pmatrix},\ a=\begin{pmatrix}-1 & 1\\ 0 & 0\end{pmatrix},\ b=\begin{pmatrix}-1 & -1\\ 0 & 0\end{pmatrix}.$$

代数运算是矩阵的普通乘法，即

	e_1	e_2	a	b
e_1	e_1	e_2	a	b
e_2	e_1	e_2	a	b
a	b	a	e_2	e_1
b	b	a	e_2	e_1

矩阵乘法满足结合律．G 里至少存在一个左单位元 e_1，使得 $e_1x=x$，$\forall x\in G$. 而且，对于 $e_1\in G$，$\exists e_1\in G$，使得 $e_1 e_1=e_1$；对于 $e_2\in G$，$\exists e_1\in G$，使得 $e_2e_1=e_1$；对于 $a\in G$，$\exists b\in G$，使得 $ab=e_1$；对于 $b\in G$，$\exists b\in G$，使得 $bb=e_1$. 即 $\forall x\in G$，$\exists x$ 的右逆元 $y\in G$，使得 $xy=e_1$. 但 G 不是一个群．因为对于 $e_2\in G$，$\overline{\exists} e_2$ 的左逆元 $z\in G$，使得 $ze_2=e_1$.

例 4 设 $G=\left\{\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}\middle|\, a,b \text{ 是实数}, a\neq 0\right\}$，代数运算是矩阵乘法．矩阵乘法适合结合律. G 有左单位元 $\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$，使得 $\forall \begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}\in G$，$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}=\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}$. $\forall \begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}\in G$，$\exists$ 右逆元 $\begin{pmatrix}\frac{1}{a} & 0\\ 0 & 0\end{pmatrix}\in G$，使得 $\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}\begin{pmatrix}\frac{1}{a} & 0\\ 0 & 0\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$. 因此 G 满足全部题设条件．但 G 不是一个群．事实上，设 c 是非零实数，则对于 $\begin{pmatrix}0 & c\\ 0 & 0\end{pmatrix}\in G$，$\forall \begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}\in G$，都有 $\begin{pmatrix}0 & c\\ 0 & 0\end{pmatrix}\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}\neq\begin{pmatrix}0 & c\\ 0 & 0\end{pmatrix}$，从而 G 中任一元都不是 G 的右单位元，即 G 没有单位元.

3. 设 G 是非交换群，且 G 的阶 $|G|>2$，证明：在 G 中除单位元 e 以外，还存在两个不同的元素 a,b，使得 $ab=ba$.

证 因 G 是非交换群，故 $\exists a\in G$，使得 $a^{-1}\neq a$（不然，若 $\forall a\in G$，都有 $a^{-1}=a$，则 $a^2=e$. 由第四章，二，4，G 是交换群）. 取 $b=a^{-1}$，则 $ab=a\,a^{-1}=a^{-1}\,a=b\,a$，且 $a\neq e,b\neq e,a\neq b$.

4. 在群里，

1） 有限阶元与有限阶元的积可能是无限阶元吗？

2） 无限阶元与无限阶元的积可能是有限阶元吗？

解 1） 有可能.

例 $G=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\middle|\, a,b,c,d \text{ 是实数}, \begin{vmatrix}a & b\\ c & d\end{vmatrix}\neq 0\right\}$ 对矩阵乘法作成一个群. 单位元是 $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$. 因

$$\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\quad \begin{pmatrix}1 & 0\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 1 & -1\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}.$$

故$\left|\begin{pmatrix}1 & 1\\0 & -1\end{pmatrix}\right|=\left|\begin{pmatrix}1 & 0\\1 & -1\end{pmatrix}\right|=2$. 但$\begin{pmatrix}1 & 0\\1 & -1\end{pmatrix}\begin{pmatrix}1 & 1\\0 & -1\end{pmatrix}=\begin{pmatrix}1 & 1\\1 & 2\end{pmatrix}$，而对于$\begin{pmatrix}1 & 1\\1 & 2\end{pmatrix}$，不存在正整数$n$，使$\begin{pmatrix}1 & 1\\1 & 2\end{pmatrix}^n=\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$，因此，$\left|\begin{pmatrix}1 & 1\\1 & 2\end{pmatrix}\right|=\infty$.

2）　有可能.

例　全体非零有理数的集合$\mathbf{Q}^*$对于普通乘法作成一个群．单位元是1. $|2|=\infty$，$\left|-\frac{1}{2}\right|=\infty$，但$\left|2\cdot\left(-\frac{1}{2}\right)\right|=|-1|=2$.

5. 设a,b是群G的任意两个元素，证明：ab与ba的阶相同.

证一　设$|ab|=s$，则$(ab)^s=e$，从而$(ab)^{s-1}(ab)=e$，于是$(ab)^{s-1}=b^{-1}a^{-1}$.

$$\begin{aligned}(ba)^s&=\overbrace{(ba)(ba)\cdots(ba)}^{s\text{个}}=b\overbrace{(ab)(ab)\cdots(ab)}^{(s-1)\text{个}}a\\&=b(ab)^{s-1}a=b(b^{-1}a^{-1})a=(bb^{-1})(a^{-1}a)\\&=e.\end{aligned}$$

$\forall$正整数$t<s$，$(ba)^t\neq e$. 不然，若$(ba)^t=e$，同理，$(ba)^{t-1}=a^{-1}b^{-1}$，$(ab)^t=a(ba)^{t-1}\cdot b=a(a^{-1}b^{-1})b=e$，但$0<t<s$，此与$|ab|=s$矛盾．所以$|ba|=s$.

设$|ab|=\infty$，则$|ba|=\infty$. 不然，若$|ba|$有限，设$|ba|=n$，同理可证$|ab|=n$. 此与假设矛盾.

证二　设$|ab|=n$，则$(ab)^n=e$，从而

$$\begin{aligned}(ba)^n&=(a^{-1}a)(ba)^n=(a^{-1}a)\overbrace{(ba)(ba)\cdots(ba)}^{n\text{个}}\\&=a^{-1}(ab)^na=a^{-1}ea=e.\end{aligned}$$

所以ba也是有限阶的，设$|ba|=m$，则$m|n$. 同理，由$(ba)^m=e$可推出$(ab)^m=e$，于是$n|m$. 由于m与n都是正整数，所以$m=n$. 因此，$|ab|=|ba|$.

证三　设$|ab|=s$，则$(ab)^s=e$，又

$$\begin{aligned}(ab)^s&=\overbrace{(ab)(ab)\cdots(ab)}^{s\text{个}}=a\overbrace{(ba)(ba)\cdots(ba)}^{(s-1)\text{个}}b\\&=a(ba)^{s-1}b,\end{aligned}$$

从而

$$a(ba)^{s-1}b=e.$$

即$(ba)^{s-1}=a^{-1}b^{-1}$，所以

$$(ba)^s=(ba)^{s-1}(ba)=(a^{-1}b^{-1})(ba)=e.$$

对于任一正整数$t<s$，必有$(ba)^t\neq e$. 不然，若$(ba)^t=e$，则

$$e=(ba)^t=\overbrace{(ba)(ba)\cdots(ba)}^{t\text{个}}=b(ab)^{t-1}a.$$

于是

$$(ab)^{t-1}=b^{-1}a^{-1}.$$

所以

$$(ab)^t=(ab)^{t-1}(ab)=b^{-1}a^{-1}ab=e.$$

但$0<t<s$，此与$|ab|=s$矛盾．所以$|ba|=e$.

注　在任意群中，abc,bca,cab同阶．事实上，$|abc|=|a(bc)|=|(bc)a|=|bca|$，$|abc|$

$=|(ab)c|=|c(ab)|=|cab|$.

6. 下面各命题是否正确,其中 G 是一个群.

1) $a,b\in G,a\neq b\Rightarrow |a^{-1}|\neq|b^{-1}|$.

2) $|a|=|a'|,|b|=|b'|\Rightarrow |ab|=|a'b'|$.

3) $|ab|=|a^{-1}b^{-1}|$.

4) $a\in G$,e 是 G 的单位元,$a^m=e,a^n=e,n|m\Rightarrow |a|=m$.

5) 设 $a\in G$,m,n 是正整数,$|a|=mn$,则

$$|a^m|=n.$$

解 1) 不正确.

例 $U_3=\{x\,|\,x$是复数$,x^3=1\}$对于复数乘法作成一个群.$\varepsilon_1=\dfrac{-1+\sqrt{3}\,\mathrm{i}}{2}$,$\varepsilon_2=\dfrac{-1-\sqrt{3}\,\mathrm{i}}{2}\in U_3$,$\varepsilon_1\neq\varepsilon_2$,但 $\varepsilon_1^{-1}=\varepsilon_2,\varepsilon_2^{-1}=\varepsilon_1,|\varepsilon_1^{-1}|=|\varepsilon_2^{-1}|=3$.

2) 不正确.

例 $U_4=\{1,-1,i,-i\}$是四次单位根群.$|i|=|-i|=4$,当然$|i|=|i|=4$,但

$$|i\,i|=|-1|=2,\quad |-i\,i|=|1|=1.$$

所以

$$|i\,i|\neq|-i\,i|.$$

3) 正确.

证 $|ab|=|(ab)^{-1}|=|b^{-1}a^{-1}|=|a^{-1}b^{-1}|$.

4) 不正确.

例 $\mathbb{Q}^*$是非零有理数对于数的乘法作成的群.1 是$\mathbb{Q}^*$的单位元.$-1\in\mathbb{Q}^*$.$(-1)^8=1,(-1)^4=1,4|8$,但$|-1|=2\neq4$.

5) 正确.

证 因 $a^{mn}=e$,故$(a^m)^n=e$.

设$(a^m)^t=e$,其中 t 是正整数,则 $a^{mt}=e$. 因$|a|=mn$,故 $mn|mt$,从而 $n|t$. 因 $t\neq0$,故 $t\geqslant n$,所以$|a^m|=n$.

7. 设非空集 A 对于乘法封闭.下面各命题是否正确.

1) $\forall a,b\in A$,方程 $ax=b$ 在 A 中有解.

2) $\forall a,b\in A$,方程 $ax=b$ 在 A 中只有一个解.

解 不正确.

1) $A=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\middle|\,a,b,c,d\in\mathbb{Z}\right\}$对于矩阵乘法封闭.方程$\begin{pmatrix}1&0\\0&0\end{pmatrix}x=\begin{pmatrix}1&0\\0&1\end{pmatrix}$在 A 中无解,因为$\begin{pmatrix}1&0\\0&0\end{pmatrix}$不是可逆矩阵.

2) $A=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\middle|\,a,b,c,d\in\mathbb{Z}\right\}$对于矩阵乘法封闭.方程$\begin{pmatrix}1&0\\0&0\end{pmatrix}x=\begin{pmatrix}2&0\\0&0\end{pmatrix}$在 A 中的解不唯一.$\begin{pmatrix}2&0\\0&0\end{pmatrix}$,$\begin{pmatrix}2&0\\1&0\end{pmatrix}$都是方程的解.实际上,方程有无穷多个解.

四、思考问题

1. 判断下列各集合对于所规定的法则$\circ$来说是否作成一个群.

1)　$\mathbb{Q}^*$是全体不等于零的有理数集．$a\circ b=-ab$.

2)　$\mathbb{Q}^*$是全体正有理数集．$a\circ b=\frac{1}{2}ab$.

3)　$\mathbb{Q}^*$是一切不等于零的有理数集．$a\circ b=-nab$,其中n是固定的正整数.

4)　$\mathbb{R}$是实数集．$a\circ b=\frac{1}{2}(a+b)$.

5)　$\mathbb{R}$是实数集．$a\circ b=a+2b$.

6)　已知G对于代数运算$\cdot$作成群．G对于$a\circ b=b\cdot a$.

7)　G对于代数运算$\cdot$作成群．u是G中的一个固定元．G对于$a\circ b=a\cdot u\cdot b$.

8)　$\mathbb{Z}$是整数集．$a\circ b=a+b-2$.

9)　$\mathbb{Z}$是整数集．$a\circ b=a+b-3$.

10)　$\mathbb{Q}-\{-1\}$对于$a\circ b=a+b+ab$.

11)　$\mathbb{Z}$是整数集．$a\circ b=a+b+2ab$.

12)　$\mathbb{R}^*$是非零实数集．$a\circ b=\begin{cases}ab, & a>0;\\ \dfrac{a}{b}, & a<0.\end{cases}$

13)　$G=\left\{t,\frac{1}{t},1-t,\frac{1}{1-t},\frac{1-t}{t},\frac{t}{1-t}\,\middle|\,t\text{是有意义的变量}\right\}$.$\circ$:以第二个因子替换第一个因子中的$t$.

14)　$\mathbb{R}^{(2)}=\mathbb{R}\times\mathbb{R}=\{(a,b)\mid a,b\in\mathbb{R}\}$.$(a_1,b_1)\circ(a_2,b_2)=(a_1+a_2,b_1+b_2)$.

15)　已知G对代数运算$\cdot$作成一个群．$G\times G$对于$(a_1,b_1)\circ(a_2,b_2)=(a_1\cdot a_2,b_1\cdot b_2)$.

16)　$G=\{(a,b)\mid a,b\text{是实数}\}$.$(a_1,b_1)\circ(a_2,b_2)=(a_1+a_2e^{-b_1},b_1+b_2)$,其中$\mathrm{e}=2.71828\cdots$.

17)　设A是一个非空集合,$P(A)=\{A\text{的一切子集}\}$.$A_1\circ B_1=A_1\cup B_1$.

18)　设A是一个非空集合,$P(A)=\{A\text{的一切子集}\}$.$A_1\circ B_1=A_1\cap B_1$.

19)　设G对于代数运算$\cdot$作成一个群,u是G的一个固定元素．G对于$a\circ b=a\cdot u^{-1}\cdot b$.

20)　设G是有理数域上全部非零多项式的集合．$\circ$是多项式的乘法.

21)　设S是任意集合,G对加法作成一个群,A是S到G的所有映射作成的集合．A对于$(f\circ g)(x)=f(x)+g(x)$.

22)　$G=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\begin{pmatrix}1&0\\0&-1\end{pmatrix},\begin{pmatrix}-1&0\\0&1\end{pmatrix}\right\}$.$\circ$是矩阵乘法.

23)　$G=\left\{e=\begin{pmatrix}1&0\\0&1\end{pmatrix},a=\begin{pmatrix}-1&0\\0&1\end{pmatrix},b=\begin{pmatrix}\frac{1}{2}&-\frac{\sqrt{3}}{2}\\-\frac{\sqrt{3}}{2}&-\frac{1}{2}\end{pmatrix},c=\begin{pmatrix}\frac{1}{2}&\frac{\sqrt{3}}{2}\\\frac{\sqrt{3}}{2}&-\frac{1}{2}\end{pmatrix},d=\begin{pmatrix}-\frac{1}{2}&\frac{\sqrt{3}}{2}\\-\frac{\sqrt{3}}{2}&-\frac{1}{2}\end{pmatrix},\right.$

$$f=\begin{pmatrix}-\frac{1}{2} & -\frac{\sqrt{3}}{2}\\ \frac{\sqrt{3}}{2} & -\frac{1}{2}\end{pmatrix}\Bigg\}.$$ ∘ 是矩阵乘法.

24） $G=\left\{\begin{pmatrix}a & 0\\ 0 & 0\end{pmatrix}\middle| a\text{ 是非零实数}\right\}$. ∘ 是矩阵乘法.

25） $G=\left\{\begin{pmatrix}a & 2b\\ b & a\end{pmatrix}\middle| a,b\in\text{数域 }F\right\}$. ∘ 是矩阵加法.

26） $G=\left\{\begin{pmatrix}a & 2b\\ b & a\end{pmatrix}\middle| a,b\in\text{数域 }F\right\}$. ∘ 是矩阵乘法.

27） $G=\left\{e=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}, a=\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}, b=\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}, c=\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}, d=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix},\right.$

$\left.f=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}\right\}$. ∘ 是矩阵乘法.

28） $G=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\middle| a,b,c,d\text{ 都是整数}, \begin{vmatrix}a & b\\ c & d\end{vmatrix}\neq 0\right\}$. ∘ 是矩阵加法.

29） G 是全体 n 阶实矩阵的集合. ∘ 是矩阵加法.

30） G 是 n 维向量空间，∘ 是向量加法.

31） 设 $A=\{a,b\}$，$P(A)=\{\varnothing,\{a\},\{b\},A\}$. $X\circ Y=(X-Y)\cup(Y-X)$.

32） $G=\{f_1(x),f_2(x),f_3(x),f_4(x),f_5(x),f_6(x)\}$，其中 $f_1(x)=x$，$f_2(x)=\frac{1}{1-x}$，$f_3(x)=\frac{x-1}{x}$，$f_4(x)=\frac{1}{x}$，$f_5(x)=1-x$，$f_6(x)=\frac{x}{x-1}$. $f_i(x)\circ f_j(x)=f_i(f_j(x))$.

33） $G=\{1,2,3,4,6,12\}$. $a\circ b=(a,b)$（a,b 的最大公因数）.

34） $\mathbb{Z}$ 是整数集.

$$a\circ b=\begin{cases}a+b, & \text{当 } a \text{ 是偶数时},\\ a-b, & \text{当 } a \text{ 是奇数时}.\end{cases}$$

35） $G=\left\{\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix},\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix},\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix},\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix}\right\}$.

∘ 是矩阵乘法.

2. 假设非空集合 G 对于所定义的乘法封闭，并满足如下各条件.

1） $\exists e\in G$，使得 $\forall a(\neq e)\in G$，都有

$$ae=a.$$

2） $\forall a,b,c(\neq e)\in G$，都有

$$a(bc)=(ab)c.$$

3） $\forall a(\neq e)\in G$，$\exists a'\in G$，使得

$$aa' = e.$$

证明：G 对这个乘法作成一个群.

3. 设非空集合 G 有一个代数运算(叫做乘法)，这个乘法适合结合律．$\forall a,b\in G$，方程 $ax=b$ 在 G 中有解，方程 $ya=a$ 在 G 中有唯一解．证明：G 是一个群.

4. 设 G 是一个群，则

$$G\text{ 是交换群} \Leftrightarrow \forall a,b\in G,\text{有}(ab)^2=a^2b^2.$$

5. 设 $a\in$ 群 G，证明：

$$a^2 = a \Leftrightarrow a = e.$$

6. 设 $a,b,c\in$ 群 G，证明：方程

$$xaxba=xbc$$

在 G 中有且仅有一个解.

7. 设 $a,b\in$ 群 G，证明：

$$(a^{-1}ba)^k=a^{-1}ba \Leftrightarrow b^k=b.$$

8. 设群 G 只有唯一的一个阶为 2 的元 a，证明：$\forall x\in G$，都有 $ax=xa$.

9. 设非空集合 G 对于$\circ$封闭，$\circ$适合结合律，有单位元 e. 对于 G 中两个元 a,b，若 $a\circ b=b\circ a$，且 $\exists b^{-1}\in G$，使得 $b\circ b^{-1}=b^{-1}\circ b=e$，证明：$b^{-1}\circ a=a\circ b^{-1}$.

10. 设 $a,b\in$ 群 G，且 $a\neq e$，$a^4b=ba^5$．证明：$ab\neq ba$.

11. 设 G 是一个群，且 G 有一个单射变换 τ，τ 也是 G 到 G 的同态映射，使 $x^{\tau}=x^3$，$\forall x\in G$. 证明：G 是交换群．

第五章　群的同态、变换群

一、基本问题问答

1. 将命题："假定群 G 与不空集合 $\overline{G}$ 对于它们的乘法来说同态，那么 $\overline{G}$ 也是一个群"改为如下命题："设

1)　G 是一个群；

2)　$\overline{G}$ 是有一个代数运算(叫乘法)的非空集合；

3)　存在 G 到 $\overline{G}$ 的一个单射的同态映射.

则 $\overline{G}$ 也是一个群."

是否仍正确？

答　不正确.

例　$G=\{e\}$ 对于 $ee=e$ 作成一个群. $\overline{G}$ 是非零整数集，普通乘法是 $\overline{G}$ 的一个代数运算.

$$\phi: e \to 1$$

是 G 到 $\overline{G}$ 的一个单射. 且

$$\phi: e \to 1,$$
$$e \to 1$$
$$\Rightarrow ee = e \to 1 = 1 \cdot 1.$$

即

$$\phi(ee) = \phi(e)\,\phi(e),$$

从而 ϕ 是 G 到 $\overline{G}$ 的单射的同态映射. 但 $\overline{G}$ 不是群，因 $2(\in \overline{G})$ 在 $\overline{G}$ 中无逆元.

2. 命题："设 ϕ 是群 G 到群 $\overline{G}$ 的一个同态映射，则

1)　G 的单位元 e 在 ϕ 下的象 $\phi(e)$ 是 $\overline{G}$ 的单位元；

2)　G 的元 a 的逆元 a^{-1} 在 ϕ 下的象 $\phi(a^{-1})$ 是 a 的象 $\phi(a)$ 的逆元."

是否成立？

答　成立. 证明如下.

1)

$$\phi: e \to \phi(e).$$

因 ϕ 保持运算，故

$$\phi: ee \to \phi(e)\,\phi(e).$$

又因 $ee=e$，且 ϕ 是映射，故 $\phi(e)\phi(e)=\phi(e)$.

设 $\bar{e}$ 是 $\overline{G}$ 的单位元，则 $\phi(e)\phi(e)=\phi(e)=\phi(e)\bar{e}$，因 $\overline{G}$ 是群，消去律Ⅲ′成立，故 $\phi(e)=\bar{e}$.

2)　因为 $\phi(a)\phi(a^{-1})=\phi(aa^{-1})=\phi(e)$，又由 1) 知 $\phi(e)$ 是 $\overline{G}$ 的单位元，所

以$(\phi(a))^{-1}=\phi(a^{-1})$.

注　还可利用子群来证明1).

作$G'=\{\phi(x)\mid x\in G\}$,则$\phi$是$G$到$G'$的同态满射.因此$\phi(e)$是$G'$的单位元[①].又因$G$是群,故$G'$也是群[②].且$G'\subset\overline{G}$.$G'$与$\overline{G}$的代数运算一样,从而由定义,$G'$是$\overline{G}$的子群.于是$G'$的单位元$\phi(e)$是$\overline{G}$的单位元$\bar{e}$[③].所以$\phi(e)=\bar{e}$.

3. 设集A中含有n个元素,则A的变换共有多少个?A的一一变换共有多少个?

答　A的变换共有n^n个.A的一一变换共有$n!$个.

4. 设$A=\{1,2\}$,则

$$\begin{aligned}\tau_1:&\quad 1\to 1,\quad 2\to 1;\\ \tau_2:&\quad 1\to 2,\quad 2\to 2;\\ \tau_3:&\quad 1\to 1,\quad 2\to 2;\\ \tau_4:&\quad 1\to 2,\quad 2\to 1\end{aligned}$$

是A的所有变换.τ_3是A的恒等变换,τ_3,τ_4是A的一一变换,τ_1,τ_2是A的非一一变换.问$\{\tau_4\},\{\tau_1,\tau_2\},\{\tau_1,\tau_3\},\{\tau_1,\tau_4\},\{\tau_3,\tau_4\},\{\tau_1\},\{\tau_2\},\{\tau_3\},\{\tau_2,\tau_3,\tau_4\},\{\tau_1,\tau_2,\tau_4\}$是不是群?若是群,是不是变换群?

答　$\{\tau_3\},\{\tau_3,\tau_4\},\{\tau_1\},\{\tau_2\}$是群.其余的不是.$\{\tau_3\},\{\tau_3,\tau_4\}$是变换群,$\{\tau_1\},\{\tau_2\}$不是变换群.

注　1)　$\{\tau_3\}$是A的最小的变换群,$\{\tau_3,\tau_4\}$是A的最大的变换群.

2)　由变换作成的群未必是变换群.如$\{\tau_1\},\{\tau_2\}$并不是由A的一一变换作成的群.

3)　$\{\tau_1,\tau_3\},\{\tau_2,\tau_3,\tau_4\}$不是群[④].

4)　由变换作成的群未必包含恒等变换,因而它的单位元未必是恒等变换.如$\{\tau_1\}$,$\{\tau_2\}$.又如A是一个至少含2个元素的集合.取定$a\in A$,$\forall x\in A$,令

$$\tau:\quad x\to a.$$

则

$$x^{\tau\tau}=(x^{\tau})^{\tau}=a^{\tau}=a=x^{\tau}.$$

所以,$\tau\tau=\tau$,从而$\{\tau\}$是一个由变换作成的群,但不是变换群.如果由变换作成的群中包含恒等变换,那么它的单位元一定是恒等变换,如$\{\tau_3\},\{\tau_3,\tau_4\}$.(见第五章,二,5.)

5)　可以证明.设

① G是非空集合A的若干变换的集合;

② G对变换乘法作成一个群;

③ A的恒等变换$\varepsilon\overline{\in}G$,

则G只含A的非一一变换.

由此性质立刻得知$\{\tau_1,\tau_4\}$和$\{\tau_1,\tau_2,\tau_4\}$都不是群.

下面我们证明这个命题.

---

① 张禾瑞.近世代数基础.北京:高等教育出版社,1978.43.定理2.

② 同上,40.定理1.

③ 同上,63.推论.

④ 同上,46.定理1.

证一 （反证法）若$\exists \tau\in G$，而τ是A的一一变换．因为G是群，所以$\forall \sigma\in G$，方程$\sigma x=\tau$，$y\sigma=\tau$在G中都有解，从而$\exists \sigma',\sigma''\in G$，使得$\sigma\sigma'=\tau,\sigma''\sigma=\tau$．

（i） σ是满射变换．事实上，$\forall a\in A$，$a=a^{\varepsilon}$．因τ是A的一一变换，故τ有逆变换τ^{-1}，使$\tau^{-1}\tau=\varepsilon$，从而

$$a=a^{\varepsilon}=a^{\tau^{-1}\tau}=a^{\tau^{-1}\sigma''\sigma}=((a^{\tau^{-1}})^{\sigma''})^{\sigma},$$

其中$a^{\tau^{-1}}\in A$．因此$\exists (a^{\tau^{-1}})^{\sigma''}\in A$，使得$((a^{\tau^{-1}})^{\sigma''})^{\sigma}=a$．所以$\sigma$是满射变换．

（ii） σ是单射变换．事实上，$\forall a,b\in A$，若$a^{\sigma}=b^{\sigma}$，则$a^{\sigma\sigma'}=b^{\sigma\sigma'}$，从而$a^{\tau}=b^{\tau}$．因$\tau$是$A$的一一变换，故$a=b$，所以$\sigma$是单射变换．

于是σ是A的一一变换，从而G是A的所有的一一变换关于变换乘法作成的群的子群．所以G包含这个A的最大变换群的单位元，而单位元是A的恒等变换ε，即$\varepsilon\in G$．此与题设矛盾．

（此证明说明：若群G中含有一个A的一一变换，则G中每个元都是A的一一变换．）

证二 （反证法）不然，若$\exists \tau\in G$，τ是A的一一变换，则$H=(\tau)\leqslant G$，且H是A的一个变换群．所以由第五章，二，5，H的单位元就是A的恒等变换ε，即$\varepsilon\in H$，从而$\varepsilon\in G$．此与已知条件矛盾．所以G中只含A的非一一变换．

证三 （反证法）不然，若$\exists \tau\in G$，使得τ是A的一个一一变换．设ε'是G的单位元，则$\varepsilon'\tau=\tau$．$\forall x\in A$，$x^{\varepsilon'\tau}=x^{\tau}$，即$(x^{\varepsilon'})^{\tau}=x^{\tau}$．因$\tau$是单射，故$x^{\varepsilon'}=x$，$\forall x\in A$．从而$\varepsilon'$是$A$的恒等变换，且$\varepsilon'\in G$，此与已知条件矛盾．于是$G$只含$A$的非一一变换．

证四 设$\tau\in G$．因G是群，故存在G的单位元$e\in G$，存在τ的逆元$\tau^{-1}\in G$，且有$\tau\tau^{-1}=\tau^{-1}\tau=e$．

假设τ是A的一一变换，从而τ有逆变换τ'（τ'未必$\in G$），且有$\tau'\tau=\varepsilon$，ε是A的恒等变换．则

$$\begin{aligned}\tau\tau^{-1}=e &\Rightarrow \tau'\tau\tau^{-1}=\tau'e\\ &\Rightarrow \varepsilon\tau^{-1}=\tau'e\Rightarrow\tau^{-1}=\tau'e\Rightarrow\tau^{-1}\tau=\tau'e\tau\\ &\Rightarrow e=\tau'\tau=\varepsilon\Rightarrow\varepsilon\in G.\end{aligned}$$

此与题设矛盾．所以G只含A的非一一变换．

6） 由注5)可知：设

① G是非空集合A的若干变换的集合；

② G对变换乘法作成一个群，

则

$$\varepsilon\in G\Leftrightarrow G\text{是}A\text{的变换群}^{①}.$$

由此性质得知，没有一个既有一一变换又有非一一变换作为元素的混杂的群．

7） 若G是A的变换群，则G的单位元是A的恒等变换ε（见第五章，二，5），G的每一个元τ的逆元τ^{-1}是τ的逆变换．若由A的变换作成的群G不是A的变换群，则G的单位元不是A的恒等变换，G的每一元τ的逆元τ^{-1}不是τ的逆变换．此时，τ根本不存在逆变换．

5. 设$G=\{e,a,b\}$是一个3阶群．利用Cayley定理：任何一个群都同一个变换群同构[②]，找出一个与G同构的变换群．

---

① 张禾瑞．近世代数基础．北京：高等教育出版社，1978．46．定理1．

② 同上，49．定理3．

答　$\forall g \in G$，作变换

$$\tau_e: \quad g \to ge = g^{\tau_e},$$
$$\tau_a: \quad g \to ga = g^{\tau_a},$$
$$\tau_b: \quad g \to gb = g^{\tau_b}.$$

作变换的集合 $\overline{G}=\{\tau_e, \tau_a, \tau_b\}$，则

$$\phi: \quad e \to \tau_e,$$
$$a \to \tau_a,$$
$$b \to \tau_b$$

是 G 与 $\overline{G}$ 间的对于 G 的乘法与变换乘法来说的同构映射. 因 G 是群，故 $\overline{G}$ 是群. 因

$$\tau_e: \quad g \to ge = g^{\tau_e} = g.$$

故 τ_e 是 G 的恒等变换，且 $\tau_e \in \overline{G}$. 从而 $\overline{G}$ 是 G 的变换群. 所以 G 与 G 的变换群 $\overline{G}$ 同构.

二、典型问题分析

1. 假定在两个群 G 和 $\overline{G}$ 的一个同态映射之下，

$$a \to \bar{a}.$$

a 与 $\bar{a}$ 的阶是不是一定相同?

解　不一定相同.

例　设 G 是整数集对于普通加法来说作成的群，$\overline{G}=\{1\}$ 是对普通乘法来说作成的群.

$$\phi: \quad n \to 1 = \phi(n)$$

是 G 到 $\overline{G}$ 的同态满射. 对于 $1 \in G$，有

$$\phi: \quad 1 \to 1 = \phi(1).$$

但 G 的元 1 的阶 $=\infty$，而 $\overline{G}$ 的元 1 的阶 $=1$. 故 1 与 $\phi(1)$ 的阶不相同.

注　1)　该命题中的“同态映射”改成“同态满射”后，a 与 $\bar{a}$ 的阶也不一定相同. 我们再举出一个例子来说明.

例　$U_4=\{1, i, -1, -i\}$ 对普通乘法作成一个群. $\overline{G}=\{1, -1\}$ 对普通乘法作成一个群.

$$\phi: \quad \pm 1 \to 1,$$
$$\pm i \to -1$$

是 U_4 到 $\overline{G}$ 的一个同态满射. U_4 中 -1 的阶是 2，但 -1 的象 1 的阶 $\neq 2$ 而 $=1$. 又 U_4 中 $\pm i$ 的阶都是 4，而它们的象 -1 的阶是 2.

2)　设 G 和 $\overline{G}$ 都是群，$\phi: a \to \bar{a}$ 是 G 到 $\overline{G}$ 的单射的同态映射，则 a 与 $\bar{a}$ 的阶相同.

证一　若 $|a|=m$，则 $a^m=e$. 设

$$\phi: \quad a \to \bar{a}.$$

因 ϕ 是同态映射，故

$$\phi: \quad a^m \to \bar{a}^m.$$

由基本问题问答 2，有

$$\phi: \quad e \to \bar{e},$$

其中 e 与 $\bar{e}$ 分别是 G 与 $\overline{G}$ 的单位元. 因 $a^m=e$，又 ϕ 是映射，故 $\bar{a}^m=\bar{e}$.

若有正整数 n，$n<m$，也使 $\bar{a}^n=\bar{e}$. 由 ϕ 是同态映射，有

$$\phi:\quad a^n \to \bar{a}^n = \bar{e}.$$

又 ϕ 是单射，从而 $a^n=e$，于是 $|a|\leqslant n<m$，此与 $|a|=m$ 矛盾. 所以 $|\bar{a}|=m$.

若 $|a|=\infty$，因 ϕ 是同态映射，故

$$\phi:\quad a^0 = e \to \bar{a}^0 = \bar{e},$$
$$a \to \bar{a},$$
$$a^2 \to \bar{a}^2,$$
$$\cdots\cdots$$

这里，$e=a^0,a,a^2,\cdots$ 互不相同，又 ϕ 是单射，从而，$\bar{e}=\bar{a}^0,\bar{a},\bar{a}^2,\cdots$ 也互不相同. 所以 $|\bar{a}|=\infty$.

证二 设 $|a|=m$，$|\bar{a}|=n$，由 ϕ 是同态映射，$\bar{a}^m=\bar{e}$，从而 $n\mid m$. 由 ϕ 是单射的同态映射，$a^n=e$，从而 $m\mid n$. 又因 m 与 n 都是正整数，故 $m=n$，即 $|a|=|\bar{a}|$.

设 $|a|=\infty$，则必 $|\bar{a}|=\infty$. 不然，若 $|\bar{a}|=n$，则 $\bar{a}^n=\bar{e}$. 由 ϕ 是单射的同态映射，有 $a^n=e$，从而 $|a|$ 有限. 此与假设矛盾. 所以 $|\bar{a}|=\infty$.

例 证明整数加群 $\mathbb{Z}$ 与非零有理数乘群 $\mathbb{Q}^*$ 不同构.

证 因为 $-1(\in\mathbb{Q}^*)$ 的阶是 2，但 $\mathbb{Z}$ 中不存在阶为 2 的元，所以 $\mathbb{Z}$ 与 $\mathbb{Q}^*$ 不同构.

3） 设 ϕ 是群 G 到群 $\overline{G}$ 的一个同态映射，$a\in G$，a 的阶有限，则由注 2)，证二知，$\phi(a)$ 的阶也有限，且 $|\phi(a)|\,\big|\,|a|$.

4） 该题解中的例也可说明，若群 $G\sim$ 群 $\overline{G}$，虽 $\overline{G}$ 是有限群，但 G 未必是有限群.

2. 假定 τ 是集合 A 的一个非一一变换. τ 会不会有一个左逆元 τ^{-1}，使得 $\tau^{-1}\tau=\varepsilon$?

分析 这是一个训练能力的很好的习题. 读者应该从理论上彻底解决这一问题. 我们可以利用 τ 有左逆元这一条件，证明 τ 是满射；同时，利用 τ 有右逆元这一条件，证明 τ 是单射①. 从而可以启发我们得出以下的五个命题.

1） 设 τ 是集 A 的一个变换，则

τ 有左逆元 τ^{-1}，使 $\tau^{-1}\tau=\varepsilon$，$\varepsilon$ 是 A 的恒等变换 $\Leftrightarrow$ τ 是 A 的满射变换.

证 $(\Rightarrow)$ $\forall a\in A$，$\exists a^{\tau^{-1}}\in A$，使得

$$(a^{\tau^{-1}})^{\tau} = a^{\tau^{-1}\tau} = a^{\varepsilon} = a.$$

所以 τ 是满射变换.

$(\Leftarrow)$ 因 τ 是 A 的满射变换，故 $\forall a\in A$，$\exists a$ 在 τ 下的逆象 $b\in A$，使得 $b^{\tau}=a$. 因 τ 未必是单射变换，故这样的 b 可能不止一个. 我们现在只取定一个 b，规定

$$\tau^{-1}:\ a \to b = a^{\tau^{-1}},\quad 若\ b^{\tau} = a,$$

则 τ^{-1} 是 A 的一个变换. $\forall a\in A$，

$$a^{\tau^{-1}\tau} = (a^{\tau^{-1}})^{\tau} = b^{\tau} = a = a^{\varepsilon},$$

从而 $\tau^{-1}\tau=\varepsilon$，$\varepsilon$ 是 A 的恒等变换.

2） 设 τ 是集 A 的一个变换，则

τ 有右逆元 τ^{-1}，使 $\tau\tau^{-1}=\varepsilon$，$\varepsilon$ 是 A 的恒等变换 $\Leftrightarrow$ τ 是 A 的单射变换.

证 $(\Rightarrow)$ $\forall a,b\in A$，$a^{\tau}=b^{\tau}\Rightarrow(a^{\tau})^{\tau^{-1}}=(b^{\tau})^{\tau^{-1}}$

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 46. 定理 1.

$$\Rightarrow a^{\tau\tau^{-1}}=b^{\tau\tau^{-1}}$$
$$\Rightarrow a^{\varepsilon}=b^{\varepsilon}$$
$$\Rightarrow a=b.$$

所以 τ 是 A 的单射变换.

（$\Leftarrow$）　$\forall a\in A$，取定 $b_1\in A$，作

$$\tau^{-1}:a\to b,\text{若}\exists b\in A,\text{使得 } b^{\tau}=a.$$
$$a\to b_1,\text{若}\bar{\exists} b\in A,\text{使得 } b^{\tau}=a.$$

$\forall a\in A$，$\exists a^{\tau}\in A$，又因 τ 是 A 的单射变换，故若 $\exists b\in A$，使得 $b^{\tau}=a$，则这样的 b 是唯一的，从而 τ^{-1} 是 A 的变换.

$\forall a\in A$，设 $a^{\tau}=x$，则 $x^{\tau^{-1}}=a\Rightarrow a^{\tau\tau^{-1}}=(a^{\tau})^{\tau^{-1}}=x^{\tau^{-1}}=a=a^{\varepsilon}$.

所以 $\tau\tau^{-1}=\varepsilon$.

3）　设 τ 是集 A 的一个变换，则

$\exists A$ 的变换 τ^{-1}，使得 $\tau^{-1}\tau=\tau\tau^{-1}=\varepsilon$，$\varepsilon$ 是 A 的恒等变换 $\Leftrightarrow\tau$ 是 A 的一一变换.

由前面的 1）与 2）可得此命题.

4）　设 A 是有限集，则 τ 是 A 的满射变换 $\Leftrightarrow\tau$ 是 A 的单射变换.

证　（$\Rightarrow$）　设 $A=\{a_1,a_2,\cdots,a_n\}$. 若 τ 不是 A 的单射变换，则必 $\exists a_1,a_2\in A,a_1\neq a_2$，但 $a_1^{\tau}=a_2^{\tau}$. 由此，A 的全部元 $a_1,a_2,\cdots,a_n$ 在 τ 下的象 $a_1^{\tau},a_2^{\tau},\cdots,a_n^{\tau}$ 至多是 $n-1$ 个不同的元，从而 A 至少有一个元在 τ 下没有逆象. 所以 τ 不是 A 的满射变换. 此与已知条件矛盾. 所以 τ 是 A 的单射变换.

（$\Leftarrow$）　设 $A=\{a_1,a_2,\cdots,a_n\}$. 因 τ 是 A 的单射变换，故 $a_1^{\tau},a_2^{\tau},\cdots,a_n^{\tau}$ 两两不同. 又 $a_1^{\tau},a_2^{\tau},\cdots,a_n^{\tau}\in A$，从而

$$\{a_1^{\tau},a_2^{\tau},\cdots,a_n^{\tau}\}=\{a_1,a_2,\cdots,a_n\}.$$

即 $\forall a_i\in A$，都 $\exists a_j\in A$，使得 $a_j^{\tau}=a_i$，从而 τ 是 A 的满射变换.

5）　若 A 是有限集，且 τ 是 A 的非一一变换，则必 $\bar{\exists}\tau^{-1}$，使得 $\tau^{-1}\tau=\varepsilon$；同时 $\bar{\exists}\tau^{-1}$，使得 $\tau\tau^{-1}=\varepsilon$，$\varepsilon$ 是 A 的恒等变换.

由前面的 4），1），2）可得此命题.

根据上面的分析，利用 1）与 5）可知：如果一个非一一变换 τ 有左逆元 τ^{-1}，使得 $\tau^{-1}\tau=\varepsilon$，$\varepsilon$ 是集 A 的恒等变换，那么 τ 必为无限集合 A 的满射变换. 下面我们举出一些例子.

例 1　设 $A=\{1,2,3,\cdots\}$.

$$\tau:n\to 1,\quad \text{当 } n=1 \text{ 时},$$
$$n\to n-1,\text{当 } n\neq 1 \text{ 时}.$$

因 $1(\in A)$ 在 τ 下的逆象有两个元：1 与 2，故 τ 不是 A 的单射变换，但 τ 是 A 的变换，且是 A 的满射变换，从而 τ 是 A 的一个非一一变换. 作

$$\tau^{-1}:n\to n+1,\text{当 } n\neq 1 \text{ 时},$$
$$n\to 1,\quad \text{当 } n=1 \text{ 时}.$$

$\forall n\in A$，

$$n=1\text{ 时},n^{\tau^{-1}\tau}=(n^{\tau^{-1}})^{\tau}=n^{\tau}=1=n^{\varepsilon},$$
$$n\neq 1\text{ 时},n^{\tau^{-1}\tau}=(n^{\tau^{-1}})^{\tau}=(n+1)^{\tau}=n=n^{\varepsilon},$$

其中 ε 是 A 的恒等变换，所以 τ 有一个左逆元 τ^{-1}，使得 $\tau^{-1}\tau=\varepsilon$.

（还可作 $\tau^{-1}: n \to n+1$，τ^{-1} 是 A 的单射变换，此 τ^{-1} 也使 $\tau^{-1}\tau=\varepsilon$.）

例 2 设 $A=\{1,2,3,\cdots\}$.

$$\tau: 2n-1 \to n,$$
$$2n \to n.$$

因 $1(\in A)$ 在变换 τ 下的逆象有 1 与 2，故 τ 不是 A 的单射变换，而是 A 的一个满射变换. 作

$$\tau^{-1}: n \to 2n.$$

$\forall n \in A$,

$$n^{\tau^{-1}\tau} = (n^{\tau^{-1}})^{\tau} = (2n)^{\tau} = n = n^{\varepsilon},$$

其中 ε 是 A 的恒等变换. 所以 τ 有一个左逆元 τ^{-1}，使得 $\tau^{-1}\tau=\varepsilon$.

例 3 设 $A=\{1,2,3,\cdots\}$.

$$\tau: 2n \to n,$$
$$2n-1 \to 1$$

是 A 的一个满射变换，不是单射变换.

$$\tau^{-1}: n \to 2n$$

是 A 的一个单射变换，不是满射变换.

$\forall n \in A$,

$$n^{\tau^{-1}\tau} = (n^{\tau^{-1}})^{\tau} = (2n)^{\tau} = n = n^{\varepsilon}.$$

所以 $\tau^{-1}\tau=\varepsilon$.

（还可作

$$\tau^{-1}: n \to 2n, n \neq 1 \text{ 时},$$
$$1 \to 1.$$

$\forall n \in A$,

$$n \neq 1 \text{ 时}, n^{\tau^{-1}\tau} = (2n)^{\tau} = n = n^{\varepsilon},$$
$$n = 1 \text{ 时}, 1^{\tau^{-1}\tau} = (1^{\tau^{-1}})^{\tau} = 1^{\tau} = 1 = 1^{\varepsilon}.$$

所以 $\tau^{-1}\tau=\varepsilon$.）

例 4 设 $\mathbb{Z}$ 是整数集.

$$\tau: x \to \frac{x}{2}, \ x \text{ 是偶数},$$
$$x \to \frac{x+1}{2}, \ x \text{ 是奇数}$$

是 $\mathbb{Z}$ 的满射变换，但不是单射变换.

$$\tau^{-1}: x \to 2x, \ x \text{ 是偶数},$$
$$x \to 2x-1, \ x \text{ 是奇数}$$

是 $\mathbb{Z}$ 的一个单射变换，但不是满射变换（因 2 无逆象）. 容易验证，有 $\tau^{-1}\tau=\varepsilon$.

（还可规定

$$\tau^{-1}: x \to 2x,$$

也有 $\tau^{-1}\tau=\varepsilon$.）

例 5 设 $\mathbb{N}$ 是自然数集.

$$\tau: n \to \begin{cases} n, & \text{当 } n \leqslant k \text{ 时}, \\ n-k, & \text{当 } n > k \text{ 时} \end{cases}$$

是$\mathbb{N}$的满射变换，但不是单射变换.

$$\tau^{-1}: n \to \begin{cases} n, & \text{当 } n \leqslant k \text{ 时}, \\ n+k, & \text{当 } n > k \text{ 时} \end{cases}$$

是$\mathbb{N}$的一个单射变换，但不是满射变换. 有

$$\tau^{-1}\tau = \varepsilon.$$

例 6　设 $A=\{a_1, a_2, \cdots, a_\lambda, \cdots\}$. 取 λ 是一个固定的自然数. 规定

$$\tau: a_i \to a_i = a_i^\tau, \quad \text{当 } i \leqslant \lambda \text{ 时},$$
$$a_i \to a_{i-1} = a_i^\tau, \text{当 } i > \lambda \text{ 时};$$

和

$$\tau^{-1}: a_i \to a_i = a_i^{\tau^{-1}}, \quad \text{当 } i \leqslant \lambda \text{ 时},$$
$$a_i \to a_{i+1} = a_i^{\tau^{-1}}, \text{当 } i > \lambda \text{ 时}.$$

显然 τ 与 τ^{-1}都是 A 的变换. 由 $a_\lambda^\tau = a_\lambda, a_{\lambda+1}^\tau = a_\lambda$ 知，τ 不是 A 到 A 的单射，从而 τ 不是 A 的一一变换. 由

$$a_i^{\tau^{-1}\tau} = (a_i^{\tau^{-1}})^\tau = \begin{cases} a_i^\tau = a_i, & \text{当 } i \leqslant \lambda \text{ 时}, \\ a_{i+1}^\tau = a_i, & \text{当 } i > \lambda \text{ 时} \end{cases}$$

知，对任意 i，$a_i^{\tau^{-1}\tau} = a_i = a_i^\varepsilon$，$\varepsilon$ 是 A 的恒等变换. 所以 $\tau^{-1}\tau = \varepsilon$.

例 7　设 $A=\{$所有非负实数$\}$.

$$\tau: x \to (x-1)^2$$

是 A 的变换. $\forall y \in A$，令 $y=(x-1)^2$，则 $x = 1 \pm \sqrt{y}$. 因 $y \geqslant 0$，故 $\exists\, 1+\sqrt{y} \in A$，使得

$$\tau: 1+\sqrt{y} \to y.$$

所以 τ 是 A 的满射变换.

取 $x_1 = 0, x_2 = 2 \in A$，

$$\tau: x_1 \to (0-1)^2 = 1,$$
$$x_2 \to (2-1)^2 = 1.$$

虽 $x_1 \neq x_2$，但 $x_1^\tau = x_2^\tau = 1$，从而 τ 不是 A 的单射变换. 作

$$\tau^{-1}: a \to 1+\sqrt{a},$$

则因 $0 \in A$，0 在 τ^{-1}下无逆象，故 τ^{-1}不是 A 的满射变换，但 τ^{-1}是 A 的单射变换.

$\forall a \in A$，

$$a^{\tau^{-1}\tau} = (a^{\tau^{-1}})^\tau = (1+\sqrt{a})^\tau = (1+\sqrt{a}-1)^2 = a = a^\varepsilon.$$

所以 $\tau^{-1}\tau = \varepsilon$.

（还可规定

$$\tau^{-1}: x \to 1+\sqrt{x}, \quad x \geqslant 1,$$
$$x \to 1-\sqrt{x}, \quad 0 \leqslant x < 1.$$

因$\frac{3}{2}$在 τ^{-1}下无逆象，故 τ^{-1}不是 A 的满射变换，但 τ^{-1}是 A 的单射变换.

$\forall x \in A$，

当 $x\geqslant 1$ 时，$(x^{\tau^{-1}})^{\tau}=(1+\sqrt{x})^{\tau}=[(1+\sqrt{x})-1]^2=x$.

当 $0\leqslant x<1$ 时，$(x^{\tau^{-1}})^{\tau}=(1-\sqrt{x})^{\tau}=(1-\sqrt{x}-1)^2=(-\sqrt{x})^2=x$，从而 $x^{\tau^{-1}\tau}=x^{\varepsilon}$. 所以 $\tau^{-1}\tau=\varepsilon$.）

3. 假定 A 是所有实数作成的集合. 证明：所有 A 的可以写成

$$x\to ax+b,\quad a,b\text{ 是有理数},\quad a\neq 0$$

形式的变换作成一个变换群. 这个群是不是一个交换群？

证 设 $G=\{\tau_{ab}\mid \forall x\in A, x^{\tau_{ab}}=ax+b, a\neq 0, a,b\text{ 是有理数}\}$，

因 $\tau_{10}\in G$，故 $G\neq\varnothing$.

Ⅰ. $\forall \tau_{ab},\tau_{cd}\in G$，$\forall x\in A$，

$$x^{\tau_{ab}\tau_{cd}}=(x^{\tau_{ab}})^{\tau_{cd}}=c(ax+b)+d=cax+cb+d=x^{\tau_{ca,cb+d}}.$$

即

$$\tau_{ab}\tau_{cd}=\tau_{ca,cb+d}.$$

因 $c\neq 0, a\neq 0$，故 $ca\neq 0$，且 $ca, cb+d$ 是有理数，所以 $\exists|\tau_{ab}\tau_{cd}\in G$.

Ⅱ. 变换乘法适合结合律.

Ⅳ. $\exists\tau_{10}\in G$，使得 $\forall\tau_{ab}\in G$，$\tau_{10}\tau_{ab}=\tau_{ab}$.

Ⅴ. $\forall\tau_{ab}\in G$，因 $a\neq 0$，故 $\exists\tau_{\frac{1}{a},-\frac{b}{a}}\in G$，使得 $\tau_{\frac{1}{a},-\frac{b}{a}}\tau_{ab}=\tau_{10}$.

综上，G 是群.

因 τ_{10} 是 A 的恒等变换，故 G 是 A 的变换群.

因 $\tau_{11}\tau_{20}=\tau_{22}$，$\tau_{20}\tau_{11}=\tau_{21}$，故

$$\tau_{11}\tau_{20}\neq\tau_{20}\tau_{11}.$$

所以 G 不是交换群.

注 1) 本题是一个基本题，是直接按照群的定义，验证集合是群的很好的练习.

2) 我们还可以利用定义来证明 G 是一个变换群. 首先证明 G 是一个群（见上面的证明），再证明 $\forall\tau_{ab}(\in G)$ 是 A 的一一变换. 事实上，$\forall y\in A$，令 $y=ax+b$，因 $a\neq 0$，故 $x=\dfrac{y-b}{a}$，从而 $\exists\dfrac{1}{a}y-\dfrac{b}{a}\in A$，使得

$$\left(\frac{1}{a}y-\frac{b}{a}\right)^{\tau_{ab}}=a\left(\frac{1}{a}y-\frac{b}{a}\right)+b=y.$$

从而 τ_{ab} 是 A 的一个满射变换. $\forall x_1,x_2\in A$，若 $x_1^{\tau_{ab}}=x_2^{\tau_{ab}}$，则 $ax_1+b=ax_2+b$，因 $a\neq 0$，故 $x_1=x_2$，从而 τ_{ab} 是 A 的一个单射变换. 显然可见，证明集 A 的若干个变换作成的群 G 是 A 的一个变换群，只需证明 A 的恒等变换在 G 中，比起利用定义要简便一些.

3) G 是实数集 A 的所有的一一变换作成的变换群的子群.

4) A 改为是所有有理数作成的集合，命题也成立.

5) 设 $\overline{G}=\left\{(a,b)\mid a,b\text{ 是有理数}, a\neq 0\right\}$. 规定：$(a,b)=(c,d)$，当且仅当 $a=c, b=d$. 则 $\overline{G}$ 对于代数运算

$$(a,b)(c,d)=(ca,cb+d)$$

来说作成一个群，且

$$\phi:\tau_{ab}\to(a,b)$$

是 G 与 $\overline{G}$ 间的一个同构映射. 事实上，ϕ显然是 G 与 $\overline{G}$ 间的一一映射. $\forall \tau_{ab},\tau_{cd}\in G$，有

$$\phi:\tau_{ab}\to(a,b),\quad \tau_{cd}\to(c,d).$$

则

$$\phi:\tau_{ab}\tau_{cd}=\tau_{ca,cb+d}\to(ca,cb+d)=(a,b)(c,d).$$

所以 $G\overset{\phi}{\cong}\overline{G}$.

4. 假定 S 是一个集合 A 的所有变换作成的集合. 我们暂时仍用旧符号

$$\tau:\ a\to a'=\tau(a)$$

来说明一个变换 τ. 证明：我们可以用

$$\tau_1\tau_2:\ a\to\tau_1[\tau_2(a)]=\tau_1\tau_2(a)$$

来规定一个 S 的乘法，这个乘法也适合结合律，并且对于这个乘法来说 A 的恒等变换 ε 还是 S 的单位元.

证

1) S 对乘法封闭.

$$\forall \tau_1,\tau_2\in S,\forall a\in A,$$

$$\tau_1:\ a\to\tau_1(a),$$

$$\tau_2:\ a\to\tau_2(a),$$

$$\tau_1\tau_2:\ a\to(\tau_1\tau_2)(a)=\tau_1[\tau_2(a)].$$

因 $\tau_1[\tau_2(a)]$是 A 中的一个唯一确定的元素，故 $\tau_1\tau_2$ 是 A 的一个变换，从而 $\exists!\,\tau_1\tau_2\in S$.

2) S 的乘法适合结合律.

$\forall \tau_1,\tau_2,\tau_3\in S,\forall a\in A$，

$$(\tau_1\tau_2)\tau_3:\ a\to[(\tau_1\tau_2)\tau_3](a)=(\tau_1\tau_2)[\tau_3(a)]=\tau_1[\tau_2(\tau_3(a))],$$

$$\tau_1(\tau_2\tau_3):\ a\to[\tau_1(\tau_2\tau_3)](a)=\tau_1[(\tau_2\tau_3)(a)]=\tau_1[\tau_2(\tau_3(a))].$$

因此，a 在$(\tau_1\tau_2)\tau_3$ 下与在 $\tau_1(\tau_2\tau_3)$下的象相等. 所以

$$(\tau_1\tau_2)\tau_3=\tau_1(\tau_2\tau_3).$$

3) A 的恒等变换 ε 是 S 的单位元.

$\forall a\in A$，

$$\varepsilon:a\to a.$$

$\forall \tau\in S$，

$$\varepsilon\tau:a\to(\varepsilon\tau)(a)=\varepsilon[\tau(a)]=\tau(a),$$

$$\tau\varepsilon:a\to(\tau\varepsilon)(a)=\tau[\varepsilon(a)]=\tau(a).$$

因此，a 在 $\varepsilon\tau$ 下与在 $\tau\varepsilon$ 下及在 τ 下的象相等. 所以

$$\varepsilon\tau=\tau\varepsilon=\tau.$$

从而，ε 是 S 的单位元.

5. 证明：一个变换群的单位元一定是恒等变换.

证一 设 e 是集合 A 的变换群 G 的单位元，$\forall \tau\in G$，因 G 是变换群，故 τ 是满射变换，从而，$\forall a\in A$，$\exists b\in A$，使得 $b^{\tau}=a$. 于是

$$a^{e}=(b^{\tau})^{e}=b^{\tau e}=b^{\tau}=a=a^{\varepsilon}.$$

所以，$e=\varepsilon$ 是 A 的恒等变换.

证二 设e是集合A的变换群G的单位元，$\forall \tau\in G, e\tau=\tau$. $\forall a\in A$，

$$a^{e\tau}=a^{\tau},\quad a^{e\tau}=(a^{e})^{\tau},$$

从而

$$(a^{e})^{\tau}=a^{\tau}.$$

因τ是单射变换，故$a^{e}=a$，所以e是A的恒等变换.

证三 （反证法）设e是集合A的变换群G的单位元，但e不是恒等变换，则$\exists b\in A$，使得$b^{e}\neq b$. 取$\tau\in G$，对于b来说，由τ是A的满射变换，$\exists b_1\in A$，使得$b_1^{\tau}=b$. 又

$$b_1^{\tau e}=(b_1^{\tau})^{e}=b^{e}\neq b,$$

从而

$$b_1^{\tau e}\neq b_1^{\tau}.$$

即

$$\tau e\neq\tau.$$

此与e是G的单位元矛盾. 所以e是恒等变换.

注 1) 该命题的如下证法是错误的.

"恒等变换是集A的全体变换作成的集合S的单位元，又群的单位元是唯一的，故变换群的单位元只能是恒等变换."

因为还不知道恒等变换是否一定在变换群中.

2) 设G是集A的变换群，则ε是A的恒等变换$\Leftrightarrow\varepsilon$是$G$的单位元.

证 略.

3) 设G是集A的变换群，$\tau\in G$，则τ^{-1}是τ的逆变换$\Leftrightarrow\tau^{-1}$是τ的逆元.

证 τ^{-1}是τ的逆变换$\Leftrightarrow\forall a\in A,\ a^{\tau^{-1}}=b$，其中$b^{\tau}=a$

$\Leftrightarrow\forall a\in A,\ (a^{\tau^{-1}})^{\tau}=a$

$\Leftrightarrow\forall a\in A,\ a^{\tau^{-1}\tau}=a^{\varepsilon}$

$\Leftrightarrow\tau^{-1}\tau=\varepsilon$，$\varepsilon$是$G$的单位元

$\Leftrightarrow\tau^{-1}$是τ的逆元.

6. 证明：实数域上一切有逆的$n\times n$矩阵对于矩阵乘法来说，作成一个群.

证 设$G=\{A\mid A$是实数域上n阶矩阵，且$|A|\neq 0\}$. 因n阶单位矩阵$E\in G$，故$G\neq\varnothing$.

Ⅰ. $\forall A,B\in G$，$|A|\neq 0$，$|B|\neq 0$，从而

$$|AB|=|A||B|\neq 0.$$

所以$AB\in G$，即G对乘法封闭.

Ⅱ. 矩阵乘法适合结合律.

Ⅳ. n阶单位矩阵E是G的单位元.

Ⅴ. $\forall A\in G$，因$|A|\neq 0$，故$\exists A$的逆矩阵$A^{-1}\in G$，使得$A^{-1}A=E$，即A在G中有左逆元A^{-1}.

所以，G是一个群.

注 1) 当$n\geqslant 2$时，G是非交换群. 事实上，取

$$A=\begin{pmatrix}1&1&&&\\0&1&&&\\&&1&&\\&&&\ddots&\\&&&&1\end{pmatrix},\quad B=\begin{pmatrix}1&0&&&\\1&1&&&\\&&1&&\\&&&\ddots&\\&&&&1\end{pmatrix}\in G.$$

（矩阵中主对角线上的元素都是 1，其他没有注明的元素都是 0.）

有 $AB\neq BA$.

2） 记本题中的群为 $GL_n(\mathbb{R})$，称为实数域$\mathbb{R}$上 n 阶完全线性群.

3） 设 $\overline{G}$ 是全体不等于零的实数的集合，则 $\overline{G}$ 对于普通乘法来说作成一个群. 且

$$\phi:A\to|A|$$

是 G 到 $\overline{G}$ 的同态满射，所以 $G\overset{\phi}{\sim}\overline{G}$.

三、讲与练

1. 证明：设 G 与 $\overline{G}$ 是任意两个群，则必存在 G 到 $\overline{G}$ 的同态映射.

证 $\phi:x\to\bar{e}$

是 G 到 $\overline{G}$ 的一个同态映射，其中 $\bar{e}$ 是 $\overline{G}$ 的单位元. 事实上，ϕ 显然是映射. 且 $\forall x,y\in G$，有 $\phi(xy)=\bar{e}=\bar{e}\bar{e}=\phi(x)\phi(y)$.

2. 判断下面命题是否正确，若对，证明之；若错，举出反例：设 G，$\overline{G}$ 都是群，$G\overset{\phi}{\sim}\overline{G}$，则

1） $\overline{G}$ 的单位元 $\bar{e}$ 在ϕ下的逆象是 G 的单位元.

2） $\forall\bar{a}\in\overline{G}$，$\bar{a}^{-1}$在$\phi$下的逆象是 $\bar{a}$ 在ϕ下的逆象的逆元.

解 1）不对.

例 设 $\mathbb{Z}$ 是整数加群. $\overline{G}=\{0\}$对普通加法作成群.

$$\phi:a\to 0$$

是 $\mathbb{Z}$ 到 $\overline{G}$ 的一个同态满射，从而 $\mathbb{Z}\overset{\phi}{\sim}\overline{G}$. 但 $\overline{G}$ 的单位元 0 的逆象除 $\mathbb{Z}$ 的单位元 0 以外，还有许多非单位元：$\pm1,\pm2,\cdots$

2） 不对.

例 设$U_3=\{1,w,w^2\,|\,w$是三次本原单位根$\}$，$U_6=\{1,w_1,w_1^2,w_1^3,w_1^4,w_1^5\,|\,w_1$ 是六次本原单位根$\}$，U_3 与 U_6 对于乘法都作成群.

$$\phi:1\to1,\quad w_1\to1,\quad w_1^2\to w,$$
$$w_1^3\to w,\quad w_1^4\to w^2,\quad w_1^5\to w^2$$

是 U_6 到 U_3 的一个同态满射. 从而 $U_6\overset{\phi}{\sim}U_3$.

取 $\bar{a}=w$，则 $\bar{a}^{-1}=w^2$，$\bar{a}^{-1}$在ϕ下的逆象是w_1^4 与w_1^5. 而 $\bar{a}$ 在ϕ下的逆象是w_1^2,w_1^3，但$(w_1^2)^{-1}=w_1^4$，$(w_1^3)^{-1}=w_1^3$. 所以，w_1^5 不是w在ϕ下的逆象的逆元.

3. 设 G 是群. 则 G 是交换群 $\Leftrightarrow\phi:a\to a^{-1}$是 G 的自同构.

证一 （$\Rightarrow$） $\forall a\in G$，$\exists\,|\,a^{-1}\in G$，使得$\phi(a)=a^{-1}$，从而ϕ是 G 到 G 的映射. $\forall a\in G$，$\exists a^{-1}\in G$，使得$\phi(a^{-1})=(a^{-1})^{-1}=a$，从而$\phi$是 G 到 G 的满射. $\forall a,b\in G$，若 $a\neq b$，则 $a^{-1}\neq b^{-1}$，即$\phi(a)\neq\phi(b)$，从而ϕ是 G 到 G 的单射. $\forall a,b\in G$，

$$\phi(ab)=(ab)^{-1}=b^{-1}a^{-1}=a^{-1}b^{-1}=\phi(a)\phi(b),$$

从而ϕ是 G 的自同构映射.

(⇐) 已知$\phi:a\to a^{-1}$是 G 的自同构.

$\forall a,b\in G$,

$$\phi(ab)=\phi(a)\phi(b)=a^{-1}b^{-1},$$
$$\phi(ab)=(ab)^{-1}=b^{-1}a^{-1},$$

从而

$$a^{-1}b^{-1}=b^{-1}a^{-1}$$
$$\Rightarrow (a^{-1}b^{-1})^{-1}=(b^{-1}a^{-1})^{-1}$$
$$\Rightarrow ba=ab.$$

所以 G 是交换群.

证二 (⇐) 已知$\phi:a\to a^{-1}$是 G 的自同构. $\forall a,b\in G$, $\exists a^{-1},b^{-1}\in G$,使得$\phi(a^{-1})=a$, $\phi(b^{-1})=b$,从而$\phi(a^{-1}b^{-1})=\phi(a^{-1})\phi(b^{-1})=ab$;又$\phi(a^{-1}b^{-1})=\phi((ba)^{-1})=ba$. 因此 $ab=ba$. 所以 G 是交换群.

(⇒) 见证一.

注 若 G 为非交换群,则$\phi:a\to a^{-1}$未必是 G 的自同构.

例 S_3 为非交换群,ϕ: $(1\ 2)(1\ 3)\to[(1\ 2)(1\ 3)]^{-1}=(1\ 2\ 3)^{-1}=(1\ 3\ 2)\neq(1\ 2)^{-1}(1\ 3)^{-1}$,从而$\phi$不是 S_3 的自同构.

4. 设 τ 是集 A 的单射变换,λ 和 λ' 是 A 的变换. 证明:$\lambda\tau=\lambda'\tau\Leftrightarrow\lambda=\lambda'$.

证 (⇒) $\forall a\in A$,有 $a^{\lambda\tau}=a^{\lambda'\tau}$,即$(a^{\lambda})^{\tau}=(a^{\lambda'})^{\tau}$. 因 τ 是单射,故 $a^{\lambda}=a^{\lambda'}$,从而$\lambda=\lambda'$.

(⇐) 由 $\lambda=\lambda'$,显然有 $\lambda\tau=\lambda'\tau$.

5. 取定 $a\in$群 G,

$$\tau_a:\ x\to axa^{-1},\quad x\in G$$

是由 a 决定的一个法则. 证明:

1) τ_a 是 G 的一个自同构. 称 τ_a 为由元 a 决定的群 G 的内自同构.

2) G 是交换群 $\Leftrightarrow$ G 的所有的内自同构都是 G 的恒等变换.

3) $\overline{G}=\{\tau_a\,|\,a\in G\}$ 是 G 的一个变换群.

4) 对于 G 的乘法与 $\overline{G}$ 的乘法来说,

$$\phi:\ x\to\tau_x,\quad x\in G$$

不一定是 G 与 $\overline{G}$ 间的同构映射.

证 1) ① $\forall x\in G$, $\exists|\,axa^{-1}\in G$,使得

$$\tau_a:\ x\to axa^{-1},$$

从而 τ_a 是 G 到 G 的一个映射.

② $\forall x'\in G$, $\exists x=a^{-1}x'a\in G$,使得

$$\tau_a:\ x=a^{-1}x'a\to a(a^{-1}x'a)a^{-1}=x',$$

从而 τ_a 是 G 到 G 的满射.

③ $\forall x_1,x_2\in G$,若 $ax_1a^{-1}=ax_2a^{-1}$,则由群 G 的乘法适合消去律,有 $x_1=x_2$,从而 τ_a 是 G 到 G 的单射.

④ $\forall x_1,x_2\in G$,

$$\tau_a: x_1 \to a x_1 a^{-1},$$
$$x_2 \to a x_2 a^{-1},$$
$$x_1 x_2 \to a x_1 x_2 a^{-1} = (a x_1 a^{-1})(a x_2 a^{-1}).$$

综上，τ_a 是 G 的一个自同构.

2)　设 ε 是 G 的恒等变换，则 $\forall x \in G, \forall a \in G$,

$$G \text{ 是交换群} \Leftrightarrow ax = xa$$
$$\Leftrightarrow axa^{-1} = x$$
$$\Leftrightarrow x^{\tau_a} = x^{\varepsilon}$$
$$\Leftrightarrow \tau_a = \varepsilon.$$

3)　$\forall \tau_a \in \overline{G}$，由 1)知 τ_a 是 G 的一一变换.

Ⅰ. $\forall \tau_a, \tau_b \in \overline{G}, \forall x \in G$，有

$$x^{\tau_a \tau_b} = (x^{\tau_a})^{\tau_b} = (axa^{-1})^{\tau_b} = b(axa^{-1})b^{-1}$$
$$= (ba)x(ba)^{-1} = x^{\tau_{ba}}.$$

所以，$\exists | \tau_a \tau_b = \tau_{ba} \in \overline{G}$，因此，$\overline{G}$ 对乘法封闭.

Ⅱ. 变换乘法适合结合律.

Ⅳ. 因群 G 有单位元 e，故 $\overline{G}$ 有恒等变换 τ_e，τ_e 就是 $\overline{G}$ 的单位元.

Ⅴ. $\forall \tau_a \in \overline{G}$，$\exists \tau_a$ 的左逆元 $\tau_{a^{-1}} \in \overline{G}$，使得

$$\tau_{a^{-1}} \tau_a = \tau_{aa^{-1}} = \tau_e.$$

综上，$\overline{G}$ 是 G 的一个变换群.

4)　例，设 $G = \{1, -1\}$，则 G 对于乘法作成一个群.

$$\tau_1: 1 \to 1 \cdot 1 \cdot 1^{-1} = 1 \cdot 1 \cdot 1 = 1,$$
$$-1 \to 1(-1)1^{-1} = 1(-1)1 = -1.$$
$$\tau_{-1}: 1 \to (-1)1(-1)^{-1} = (-1)1(-1) = 1,$$
$$-1 \to (-1)(-1)(-1)^{-1} = (-1)(-1)(-1) = -1.$$
$$\phi: 1 \to \tau_1.$$
$$-1 \to \tau_{-1}.$$

$1 \neq -1$，但 $\tau_1 = \tau_{-1}$，从而 ϕ 不是 G 到 $\overline{G}$ 的单射，所以 ϕ 不是 G 与 $\overline{G}$ 间的同构映射.

6. 设集 A 所含的元的个数大于 1，证明：存在 A 的若干个非一一变换作成的集，它关于变换乘法作成群.

证　设 $A = \{a, b, \cdots\}$. 取定 $a \in A$，作

$$\tau: x \to a, \quad \forall x \in A.$$

由于 A 至少含两个元，从而 τ 是 A 的一个非一一变换. 因 $\tau\tau = \tau$，故 $G = \{\tau\}$ 对于变换乘法作成一个群. G 的单位元是 τ，τ 的逆元是自身.

7. 设 G 是非空集合 A 的所有的一一变换对于变换乘法作成的变换群. 若 A 含有多于两个元，证明：G 不是交换群.

证　设 $A = \{a_1, a_2, a_3, \cdots\}$,

$$\sigma: a_1 \to a_2, \quad a_2 \to a_3, \quad a_3 \to a_1.$$

而其余的 $x \in A$,

$$\sigma: x \to x.$$

$$\tau: a_1 \to a_2, \quad a_2 \to a_1, \quad a_3 \to a_3.$$

而其余的 $x \in A$，

$$\tau: x \to x.$$

则 σ, τ 是 A 的两个一一变换，从而 $\sigma, \tau \in G$. 但对于 $a_2 \in A$ 来说，

$$a_2^{\sigma\tau} = (a_2^\sigma)^\tau = a_3^\tau = a_3,$$

$$a_2^{\tau\sigma} = (a_2^\tau)^\sigma = a_1^\sigma = a_2,$$

从而

$$a_2^{\sigma\tau} \neq a_2^{\tau\sigma}.$$

所以

$$\sigma\tau \neq \tau\sigma.$$

因此 G 不是交换群.

8. 设 τ 是集 A 的一一变换，λ 是 A 的变换，证明：

1） λ 是 A 的单射变换 $\Leftrightarrow$ $\lambda\tau$ 是 A 的单射变换.

2） λ 是 A 的满射变换 $\Leftrightarrow$ $\lambda\tau$ 是 A 的满射变换.

证 1） （$\Rightarrow$） 显然 $\lambda\tau$ 是 A 的变换. $\forall a, b \in A$，若 $a \neq b$，因 λ 是 A 的单射变换，故 $a^\lambda \neq b^\lambda$. 又因 τ 是 A 的单射变换，故 $(a^\lambda)^\tau \neq (b^\lambda)^\tau$，即 $a^{\lambda\tau} \neq b^{\lambda\tau}$. 所以 $\lambda\tau$ 是 A 的单射变换.

（$\Leftarrow$） $\forall a, b \in A$，若 $a \neq b$，因 $\lambda\tau$ 是 A 的单射变换，故 $a^{\lambda\tau} \neq b^{\lambda\tau}$，即 $(a^\lambda)^\tau \neq (b^\lambda)^\tau$，因 τ 是 A 到 A 的映射，故 $a^\lambda \neq b^\lambda$. 所以 λ 是 A 的单射变换.

2） （$\Rightarrow$） 显然 $\lambda\tau$ 是 A 的变换. $\forall a'' \in A$，由 τ 是满射，$\exists a' \in A$，使得 $a'^\tau = a''$. 又由 λ 是满射，$\exists a \in A$，使得 $a^\lambda = a'$. 于是 $\exists a \in A$，使得

$$a^{\lambda\tau} = (a^\lambda)^\tau = a'^\tau = a''.$$

所以 $\lambda\tau$ 是满射.

（$\Leftarrow$） $\forall a' \in A$，因 τ 是 A 的变换，故 $\exists a'' \in A$，使得 $a'^\tau = a''$. 对于 $a'' \in A$ 来说，因 $\lambda\tau$ 是满射，故 $\exists a \in A$，使得 $a^{\lambda\tau} = a''$，从而 $a^{\lambda\tau} = a'^\tau$，即 $(a^\lambda)^\tau = a'^\tau$. 因 τ 是单射，故 $a^\lambda = a'$. 所以 λ 是满射.

四、思考问题

1. 试判断下面各命题是否正确.

1） 设 ϕ 是群 G 到群 $\overline{G}$ 的一个同态映射，$a, b \in G$，有 $\phi(a)\phi(b) = \phi(b)\phi(a)$，则 $ab = ba$.

2） 设 $\phi: x \to 2^{x-1}$ 是实数加群 $\mathbb{R}$ 到正实数乘群 $\mathbb{R}^+$ 的一个映射，则

① ϕ 是 $\mathbb{R}$ 与 $\mathbb{R}^+$ 间的一个一一映射.

② ϕ 是 $\mathbb{R}$ 与 $\mathbb{R}^+$ 间的一个同构映射.

3） 设 $\phi: n \to \begin{cases} 1, & \text{当 } 2 \mid n \text{ 时} \\ -1, & \text{当 } 2 \nmid n \text{ 时} \end{cases}$（即 $\phi(n) = (-1)^n$）是整数加群 $\mathbb{Z}$ 到非零实数乘群 $\mathbb{R}^*$ 的一个映射，则

① ϕ 是 $\mathbb{Z}$ 到 $\mathbb{R}^*$ 的一个同态映射.

② ϕ是$\mathbb{Z}$到$\mathbb{R}^*$的一个满射.

③ ϕ是$\mathbb{Z}$到$\mathbb{R}^*$的一个单射.

4) 设ϕ：$n \to \mathrm{i}^n$(i是虚数单位)是整数加群$\mathbb{Z}$到非零复数乘群$\mathbb{C}^*$的一个映射，则

① ϕ是$\mathbb{Z}$到$\mathbb{C}^*$的一个同态映射.

② ϕ是$\mathbb{Z}$到$\mathbb{C}^*$的一个满射.

③ ϕ是$\mathbb{Z}$到$\mathbb{C}^*$的一个单射.

5) 复数加群$\mathbb{C}$与非零复数乘群$\mathbb{C}^*$同构.

2. 证明下面各ϕ是群G到群$\overline{G}$的同态满射.

1) G是实数加群，$\overline{G}=\left\{z \mid z \in \mathbb{C}, |z|=1\right\}$对乘法作成一个群. $\phi: x \to \mathrm{e}^{\mathrm{i}x}$，其中e＝2.71828…

2) G是正有理数乘数，$\overline{G}$是整数加群. $\forall \alpha \in G$，都有$\alpha=2^n\alpha_1$，其中$\alpha_1(\in G)$的分子和分母均与2互素，而$n \in \overline{G}$. $\phi: \alpha \to n$.

3) G是非零有理数乘群，$\overline{G}$是正有理数乘群. $\phi: x \to |x|$.

3. 证明下面各ϕ是群G到群$\overline{G}$的同构映射.

1) $G=\left\{2k \mid k \in \mathbb{Z}\right\}$与$\overline{G}=\left\{3k \mid k \in \mathbb{Z}\right\}$对于加法都作成群. $\phi: 2k \to 3k$.

2) $G=\left\{a+b\sqrt{3} \mid a, b \in \mathbb{R}\right\}$对于加法作成一个群，$\overline{G}=\left\{(a,b) \mid a, b \in \mathbb{R}\right\}$对于$(a,b)+(c,d)=(a+c, b+d)$作成一个群. $\phi: a+b\sqrt{3} \to (a,b)$.

3) G是正实数乘群，$\overline{G}$是实数加群. $\phi: x \to \ln x$.

4) $G=\left\{a+b\sqrt{2} \mid a, b\text{ 是不同时为零的有理数}\right\}$对于数的乘法作成一个群，$\overline{G}=\left\{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \middle| a, b\text{ 是不同时为零的有理数}\right\}$对于矩阵乘法作成一个群. $\phi: a+b\sqrt{2} \to \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$.

5) G是实数加群，$\overline{G}=\left\{\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \middle| \lambda \in \mathbb{R}\right\}$对于矩阵乘法作成一个群. $\phi: \lambda \to \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$.

6) $G=\left\{\cos\theta+\mathrm{i}\sin\theta \mid \theta \in \mathbb{R}\right\}$对于数的乘法作成一个群，$\overline{G}=\left\{\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \middle| \theta \in \mathbb{R}\right\}$对于矩阵乘法作成一个群. $\phi: \cos\theta+\mathrm{i}\sin\theta \to \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.

7) $G=\left\{\tau_\theta \middle| \tau_\theta: \begin{cases} x'=x\cos\theta-y\sin\theta \\ y'=x\sin\theta+y\cos\theta \end{cases}\right\}$对于变换乘法作成一个群，$\overline{G}=\left\{\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \middle| \theta \in \mathbb{R}\right\}$对于矩阵乘法作成一个群. $\phi: \tau_\theta \to \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.

8) $G=\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b\text{ 是不全为零的实数}\right\}$对于矩阵乘法作成一个群，$\overline{G}$是非零复数乘群. $\phi: \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \to a+b\mathrm{i}$.

9) 设A是一个固定的n阶实对称矩阵. $G=\left\{P \mid P\text{ 是 }n\text{ 阶可逆实矩阵，使得 }P'AP=A\right\}$对于矩阵乘法作成一个群. 设$n$阶实对称矩阵$B$与$A$合同，即$\exists\, n$阶可逆实矩阵$C$，使得

$B=C'AC$. $\overline{G}=\left\{Q \middle| Q\text{ 是 } n \text{ 阶可逆实矩阵,使得 } Q'BQ=B\right\}$对于矩阵乘法作成一个群. $\phi: P \to C^{-1}PC$.

10) $G=\mathbb{Q}[x]$, $\overline{G}=\mathbb{Q}[x^2]$对于多项式加法都作成群. $\phi: f(x) \to f(x^2)$.

4. 找出从整数加群$\mathbb{Z}$到有理数加群$\mathbb{Q}$的所有的同态.

5. 找出整数加群$\mathbb{Z}$的所有自同态和所有自同构.($\mathbb{Z}$到$\mathbb{Z}$的同态映射称为$\mathbb{Z}$的自同态.)

6. 设群G的自同构只有恒等变换.证明:G是交换群,且$\forall x \in G$,满足$x^2=e$.

7. 设A是平面的所有点的集合,τ_θ表示平面的点绕定点转θ角的旋转,证明:$G_1=\{\tau_0, \tau_\pi\}$, $G_2=\{\tau_0, \tau_{\frac{\pi}{2}}, \tau_\pi, \tau_{\frac{3\pi}{2}}\}$都是$A$的变换群.

8. 设$a \in A$,求证:集A的所有使a不动的一一变换的集合是A的变换群.

9. 证明下列各集G对于变换乘法作成一个群.

1) $A=\{1,2,3,4,5\}$的变换

τ_1:	τ_2:	τ_3:
$1 \to 5$	$1 \to 4$	$1 \to 2$
$2 \to 2$	$2 \to 5$	$2 \to 4$
$3 \to 2$	$3 \to 5$	$3 \to 4$
$4 \to 4$	$4 \to 2$	$4 \to 5$
$5 \to 5$	$5 \to 4$	$5 \to 2$

都是A的非一一变换. $G=\{\tau_1, \tau_2, \tau_3\}$.

2) 模6的剩余类加群$\mathbb{Z}_6=\{[0],[1],[2],[3],[4],[5]\}$的变换

τ_1:	τ_2:
$[0] \to [0]$	$[0] \to [0]$
$[1] \to [4]$	$[1] \to [2]$
$[2] \to [2]$	$[2] \to [4]$
$[3] \to [0]$	$[3] \to [0]$
$[4] \to [4]$	$[4] \to [2]$
$[5] \to [2]$	$[5] \to [4]$

都是$\mathbb{Z}_6$的非一一变换. $G=\{\tau_1, \tau_2\}$.

10. 设$M_n(\mathbb{R})$是实数域$\mathbb{R}$上的一切n阶方阵的集合. $\forall A, B \in M_n(\mathbb{R})$,且$|A| \neq 0$.令

$$\tau_{A,B}: \quad X \to AX+B.$$

证明:1) $G=\left\{\tau_{A,B} \middle| A, B \in M_n(\mathbb{R}), |A| \neq 0\right\}$是$M_n(\mathbb{R})$的一个变换群.

2) $H=\left\{\tau_{I,B} \middle| I\text{ 是 } n \text{ 阶单位矩阵}, B \in M_n(\mathbb{R})\right\}$是$M_n(\mathbb{R})$的一个变换群.

3) $K=\left\{\tau_{A,0} \middle| A \in M_n(\mathbb{R}), |A| \neq 0\right\}$是$M_n(\mathbb{R})$的一个变换群.

4) 设$GL_n(\mathbb{R})$是实数域$\mathbb{R}$上的一切n阶可逆方阵的集合.则$K=\left\{\tau_{A,0} \middle| A \in GL_n(\mathbb{R})\right\}\left(=\left\{\tau_{A,0} \middle| A \in M_n(\mathbb{R}), |A| \neq 0\right\}\right)$是$GL_n(\mathbb{R})$的一个变换群.

5) $\phi: \tau_{I,B} \to B$是变换群H与加群$M_n(\mathbb{R})$间的一个同构映射.

6) $\psi: \tau_{A,0} \to A$是变换群K与乘群$GL_n(\mathbb{R})$间的一个同构映射.

11. 利用Cayley定理,找出一些变换群,使之分别与下面各群同构.

1) 整数加群$\mathbb{Z}$.

2)　实数加群$\mathbb{R}$.

3)　非零实数乘群$\mathbb{R}^*$.

4)　实数域$\mathbb{R}$上的一切n阶方阵的集合对于矩阵加法作成的群$M_n(\mathbb{R})$.

5)　实数域$\mathbb{R}$上的一切n阶可逆方阵的集合对于矩阵乘法作成的群$GL_n(\mathbb{R})$.

6)　有理数加群$\mathbb{Q}$.

7)　非零有理数乘群$\mathbb{Q}^*$.

8)　平面上所有点的集合对于加法：$(x,y)+(x',y')=(x+x',y+y')$作成的群$\pi=\left\{(x,y)\middle|x,y\in\mathbb{R}\right\}$.

第六章　置换群、循环群

一、基本问题问答

1. 1)　置换群的定义是什么?

2)　有限变换群是否为置换群?

答　1)　G是一个置换群

$\Leftrightarrow G$是一个有限集合的若干个置换作成的群

$\Leftrightarrow G$是有限集合的变换群.

2)　有限变换群未必是置换群. 例如,设π是一个平面上所有的点作成的集合,则平面上的点变到自身变换是π的一个恒等变换ε,从而$\{\varepsilon\}$是π的一个有限变换群. 但$\{\varepsilon\}$不是有限集合的变换群. 所以$\{\varepsilon\}$不是置换群.

2. 证明:每一个有限群都与一个置换群同构.

证　由 Cayley 定理的证明知,任何一个群G都与G的一个变换群$\overline{G}$同构. 今设G是有限群,从而G的一个变换群$\overline{G}$就是置换群. 所以每一个有限群都与一个置换群同构.

注　下面的证法是错误的:"由 Cayley 定理知,任何一个群都同一个变换群同构,因此,有限群G也与一个变换群$\overline{G}$同构. 则此变换群$\overline{G}$必为有限变换群,从而$\overline{G}$是一个置换群,即有限群都与一个置换群同构."因为有限变换群$\overline{G}$未必是置换群.

3. 设$a\in$群G,证明:

1)　$|a|$有限$\Leftrightarrow \exists$不同整数h与k,使得$a^h=a^k$.

2)　若$|a|$有限,且$|a|=n$,则

$$a^h=a^k \Leftrightarrow n\mid h-k,\ \forall h,k\in\mathbb{Z}.$$

3)　若$|a|=\infty$,则

$$a^h=a^k \Leftrightarrow h=k,\ \forall h,k\in\mathbb{Z}.$$

证　1)　($\Leftarrow$)　设$\exists$不同整数h与k,使得$a^h=a^k$,不妨设$h>k$,则$a^{h-k}=e$,其中$h-k$是正整数,从而$|a|$有限.

($\Rightarrow$)　若$|a|=n$为一正整数,则对于任何整数k总有$n+k\neq k$,取$h=n+k$,有$a^h=a^{n+k}=a^na^k=a^k$.

注　事实上,给定任何整数k以后,都存在无限多个h,使得$a^h=a^k$. 只要取$h=qn+k$(其中$q\in\mathbb{Z}$,$q\neq 0$)即可.

2)　($\Leftarrow$)　由$n\mid h-k$,$\exists q\in\mathbb{Z}$,使得$h-k=qn$,即$h=qn+k$. 所以$a^h=a^{qn+k}=(a^n)^qa^k=e^qa^k=a^k$.

($\Rightarrow$)　设$h-k=qn+r$,$0\leqslant r<n$,则由$a^h=a^k$,有$e=a^{h-k}=a^{qn+r}=(a^n)^qa^r=a^r$. 因$|a|$

$=n$，又 $0\leqslant r<n$，故 $r=0$，从而 $h-k=qn$，即 $n\mid h-k$.

3)　($\Leftarrow$)　显然.

($\Rightarrow$)　假设 $h\neq k$，已知 $a^h=a^k$，由 1)$\Leftarrow$知，$|a|$有限．此与已知 $|a|=\infty$ 矛盾．所以 $h=k$.

4. 我们已知重要结论：假定 G 是一个由元 a 所生成的循环群．那么 G 的构造完全可以由 a 的阶来决定：

a 的阶若是无限，那么 G 与整数加群同构；

a 的阶若是一个有限整数 n，那么 G 与模 n 的剩余类加群同构.

今证明，其逆命题也成立．即：设 $G=(a)$．1) 若 G 与整数加群 $\mathbb{Z}$ 同构，则 $|a|=\infty$；2) 若 G 与模 n 的剩余类加群 $\mathbb{Z}_n$ 同构，则 $|a|=n$.

证　1)　假设 $|a|$ 有限，设 $|a|=n$，由重要结论，$G\cong\mathbb{Z}_n$．再由已知，$\mathbb{Z}\cong\mathbb{Z}_n$，但 $|\mathbb{Z}|=\infty$，$|\mathbb{Z}_n|=n$，此为矛盾．所以 $|a|=\infty$.

2)　假设 $|a|=m\neq n$，由该结论，$G\cong\mathbb{Z}_m$，再由已知，$\mathbb{Z}_m\cong\mathbb{Z}_n$，但 $|\mathbb{Z}_m|=m$，$|\mathbb{Z}_n|=n$，此与 $m\neq n$ 矛盾．假设 $|a|=\infty$，由该结论，$G\cong\mathbb{Z}$，再由已知，$\mathbb{Z}_n\cong\mathbb{Z}$，出现矛盾，所以 $|a|=n$.

注　在同构的意义下，无限循环群只有一个．因为任一无限循环群都与整数加群 $\mathbb{Z}$ 同构，所以任意两个无限循环群必同构．有限循环群由其阶唯一决定．因为任意两个同阶有限循环群必同构.

5. 在循环群 $G=(a)$ 中，生成元 a 的阶与群 G 的阶是什么关系？

答　生成元 a 的阶＝循环群 G 的阶．具体来说，在 $G=(a)$ 中，

1)　$|a|=$ 正整数 $n\Leftrightarrow|G|=$ 正整数 n.

2)　$|a|=\infty\Leftrightarrow|G|=\infty$.

事实上，1)　($\Rightarrow$)　由 $|a|=n$ 及该结论，$G\cong\mathbb{Z}_n$，从而 $|G|=|\mathbb{Z}_n|=n$.

($\Leftarrow$)　已知 $|G|=n$，必有 $|a|$ 有限．假设不然，若 $|a|$ 无限，则由该结论，$G\cong\mathbb{Z}$，从而 G 是无限群，此与 $|G|=n$ 矛盾．所以可设 $|a|=$ 正整数 m．由必要性知 $|G|=m$．于是 $m=n$，即 $|a|=n$.

2)　命题 1)的逆否命题即命题 2).

6. 证明：若 $a\in$ 群 G，且 $|G|=|a|=n$，则 $G=(a)$.

证　已知 $|a|=n$，由上一问题 5 知，$|(a)|=n$，即 $|(a)|=|G|=n$．又 $(a)\subset G$，故 $G=(a)$.

注　设 G 是有限群，则 1)$G=(a)$；2)$|a|=n,a\in G$；3)$|G|=n$，此三者中任两个可以推出第三个.

二、典型问题分析

1. 证明：在 n 次对称群 S_n 中，

1)　两个不相连的循环置换可以交换；

2)　$(i_1\,i_2\cdots\,i_k)^{-1}=(i_k\,i_{k-1}\cdots\,i_1)$.

证一　1)　设 $i_1\,i_2\cdots\,i_k\,i_{k+1}\cdots\,i_m\,i_{m+1}\cdots\,i_n$ 是 $1,2,\cdots,n$ 的一个排列，$1\leqslant k<m\leqslant n$.

$$(i_1\ i_2\ \cdots\ i_k)(i_{k+1}\ i_{k+2}\cdots\ i_m)$$
$$=\begin{pmatrix} i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_m & i_{m+1} & \cdots & i_n \\ i_2 & i_3 & \cdots & i_1 & i_{k+1} & \cdots & i_m & i_{m+1} & \cdots & i_n \end{pmatrix}\begin{pmatrix} i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_m & i_{m+1} & \cdots & i_n \\ i_1 & i_2 & \cdots & i_k & i_{k+2} & \cdots & i_{k+1} & i_{m+1} & \cdots & i_n \end{pmatrix}$$
$$=\begin{pmatrix} i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_m & i_{m+1} & \cdots & i_n \\ i_2 & i_3 & \cdots & i_1 & i_{k+2} & \cdots & i_k & i_{m+1} & \cdots & i_n \end{pmatrix}.$$

又

$$(i_{k+1}\,i_{k+2}\ \cdots\ i_m)\ (i_1 i_2\ \cdots\ i_k)$$
$$=\begin{pmatrix} i_{k+1} & i_{k+2} & \cdots & i_m & i_1 & i_2 & \cdots & i_k & i_{m+1} & \cdots & i_n \\ i_{k+2} & i_{k+3} & \cdots & i_{k+1} & i_1 & i_2 & \cdots & i_k & i_{m+1} & \cdots & i_n \end{pmatrix}\begin{pmatrix} i_{k+1} & i_{k+2} & \cdots & i_m & i_1 & i_2 & \cdots & i_k & i_{m+1} & \cdots & i_n \\ i_{k+1} & i_{k+2} & \cdots & i_m & i_2 & i_3 & \cdots & i_1 & i_{m+1} & \cdots & i_n \end{pmatrix}$$
$$=\begin{pmatrix} i_{k+1} & i_{k+2} & \cdots & i_m & i_1 & i_2 & \cdots & i_k & i_{m+1} & \cdots & i_n \\ i_{k+2} & i_{k+3} & \cdots & i_{k+1} & i_2 & i_3 & \cdots & i_1 & i_{m+1} & \cdots & i_n \end{pmatrix}$$
$$=\begin{pmatrix} i_1 & i_2 & \cdots & i_k & i_{k+1} & i_{k+2} & \cdots & i_m & i_{m+1} & \cdots & i_n \\ i_2 & i_3 & \cdots & i_1 & i_{k+2} & i_{k+3} & \cdots & i_{k+1} & i_{m+1} & \cdots & i_n \end{pmatrix}.$$

所以

$$(i_1\ i_2\ \cdots\ i_k)\ (i_{k+1}\ i_{k+2}\cdots\ i_m)=(\ i_{k+1}\ i_{k+2}\cdots\ i_m)(i_1\ i_2\ \cdots\ i_k).$$

2)

$$(i_1\ i_2\ \cdots\ i_k)^{-1}=\begin{pmatrix} i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_n \\ i_2 & i_3 & \cdots & i_1 & i_{k+1} & \cdots & i_n \end{pmatrix}^{-1}$$
$$=\begin{pmatrix} i_2 & i_3 & \cdots & i_1 & i_{k+1} & \cdots & i_n \\ i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_n \end{pmatrix}$$
$$=\begin{pmatrix} i_k & i_{k-1} & \cdots & i_3 & i_2 & i_1 & i_{k+1} & \cdots & i_n \\ i_{k-1} & i_{k-2} & \cdots & i_2 & i_1 & i_k & i_{k+1} & \cdots & i_n \end{pmatrix}$$
$$=(i_k\,i_{k-1}\ i_{k-2}\cdots\ i_3\ i_2\ i_1).$$

证二 1) 设 π 与 π' 为两个不相连的循环置换，于是任一元素 $i\in\{1,2,\cdots,n\}$，若 i 被 π 变动，则 i 在 π' 下必不变，从而 $i^{\pi}=j\neq i$. 因此 $j^{\pi}=(i^{\pi})^{\pi}\neq i^{\pi}=j$，即 j 也是被 π 变动的元素. 因而 i,j 在 π' 下都不变. 于是有

$$i^{\pi\pi'}=(i^{\pi})^{\pi'}=j^{\pi'}=j,\ i^{\pi'\pi}=(i^{\pi'})^{\pi}=i^{\pi}=j.$$

即

$$i^{\pi\pi'}=i^{\pi'\pi}.$$

同理，对于任一被 π' 变动的元 k 也有

$$k^{\pi\pi'}=k^{\pi'\pi}.$$

而对于那些在 π 与 π' 下均不变的元素 l 来说，显然有

$$l^{\pi\pi'}=l=l^{\pi'\pi}.$$

所以 $\pi\pi'=\pi'\pi$.

2) 因为 $(i_1\ i_2\cdots\ i_k)(i_k\ i_{k-1}\cdots\ i_1)=(i_1)$ 是恒等置换，也就是 n 次对称群 S_n 的单位元，所以

$$(i_1\ i_2\cdots\ i_k)^{-1}=(i_k\,i_{k-1}\cdots\ i_1).$$

证三 1) 见证二.

2) 设 $\pi=(i_1\ i_2\cdots\ i_k)$ 是 $A=\{a_1,a_2,\cdots,a_n\}$ 的一个 n 元置换．$\forall\, a_{i_j}\in A$，$a_{i_j}^{\pi\pi^{-1}}=a_{i_j}^{\varepsilon}=a_{i_j}$，其中 ε 是 A 的恒等置换，即 S_n 的单位元.

当 $1\leqslant j<k$ 时，$a_{i_j}^{\pi\pi^{-1}}=\left(a_{i_j}^{\pi}\right)^{\pi^{-1}}=a_{i_{j+1}}^{\pi^{-1}}$，所以

$$a_{i_{j+1}}^{\pi^{-1}}=a_{i_j}.$$

当 $j=k$ 时，$a_{i_j}^{\pi\pi^{-1}}=\left(a_{i_j}^{\pi}\right)^{\pi^{-1}}=a_{i_1}^{\pi^{-1}}$，所以

$$a_{i_1}^{\pi^{-1}}=a_{i_k}.$$

当 $k+1\leqslant j\leqslant n$ 时，$a_{i_j}^{\pi\pi^{-1}}=\left(a_{i_j}^{\pi}\right)^{\pi^{-1}}=a_{i_j}^{\pi^{-1}}$，所以

$$a_{i_j}^{\pi^{-1}}=a_{i_j},$$

从而

$$\pi^{-1}=\begin{pmatrix}i_1\ i_2\cdots i_{k-1}\ i_k & i_{k+1}\cdots i_n\\ i_k\ i_1\cdots i_{k-2}\ i_{k-1} & i_{k+1}\cdots i_n\end{pmatrix}=(i_k\ i_{k-1}\ \cdots\ i_2\ i_1).$$

2. 证明：S_n 的一个 k-循环置换的阶是 k.

证一 首先证明下面命题. 设

$$\pi=(i_1\ i_2\ \cdots\ i_k)=\begin{pmatrix}i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_n\\ i_2 & i_3 & \cdots & i_1 & i_{k+1} & \cdots & i_n\end{pmatrix}$$

是 S_n 中的一个 k-循环置换，$1\leqslant l\leqslant k$，则

$$\pi^l=\begin{pmatrix}i_1 & i_2 & \cdots i_{k-l} & i_{k-l+1} & \cdots i_k & i_{k+1} & \cdots i_n\\ i_{l+1} & i_{l+2} & \cdots i_k & i_1 & \cdots i_l & i_{k+1} & \cdots i_n\end{pmatrix}.$$

下面对 l 作数学归纳法.

1) $l=1$ 时，命题显然成立.

2) 假设 $l-1$ 时，命题成立．今证 l 时，命题也成立．

$$\pi^l=\pi^{l-1}\pi$$

$$\xlongequal[\text{假设}]{\text{由归纳}}\begin{pmatrix}i_1\ i_2 & \cdots i_{k-l}\ i_{k-l+1}\ i_{k-l+2} & \cdots i_k & i_{k+1}\cdots i_n\\ i_l\ i_{l+1} & \cdots i_{k-1}\ i_k\quad i_1 & \cdots i_{l-1} & i_{k+1}\cdots i_n\end{pmatrix}\begin{pmatrix}i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_n\\ i_2 & i_3 & \cdots & i_1 & i_{k+1} & \cdots & i_n\end{pmatrix}$$

$$=\begin{pmatrix}i_1 & i_2 & \cdots i_{k-l} & i_{k-l+1} & \cdots i_k & i_{k+1} & \cdots i_n\\ i_{l+1} & i_{l+2} & \cdots i_k & i_1 & \cdots i_l & i_{k+1} & \cdots i_n\end{pmatrix}.$$

所以由归纳原理知命题成立.

当 $l=k$ 时，

$$\pi^k=\begin{pmatrix}i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_n\\ i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_n\end{pmatrix}=(1).$$

当正整数 $l<k$ 时，

$$i_1^{\pi^l}=i_{l+1}\neq i_1(\text{因 } l\neq 0).$$

即 $\pi^l\neq(1)$. 所以 $|\pi|=k$.

证二 设 $\pi=(i_1\ i_2\cdots\ i_k)$ 是 S_n 中的一个 k-循环置换，则

$$i_1^{\pi} = i_2, \quad i_1^{\pi^2} = i_3, \quad i_1^{\pi^3} = i_4, \cdots$$
$$i_2^{\pi} = i_3, \quad i_2^{\pi^2} = i_4, \quad i_2^{\pi^3} = i_5, \cdots$$
$$\vdots \qquad \vdots \qquad \vdots$$
$$i_{k-1}^{\pi} = i_k, \quad i_{k-1}^{\pi^2} = i_1, \quad i_{k-1}^{\pi^3} = i_2, \cdots$$
$$i_k^{\pi} = i_1, \quad i_k^{\pi^2} = i_2, \quad i_k^{\pi^3} = i_3, \cdots.$$

一般来说，若 $j=1,2,\cdots,k,1\leqslant l\leqslant k$，则

$$i_j^{\pi^l} = i_{l+j}, \quad l+j \leqslant k \text{ 时},$$
$$i_j^{\pi^l} = i_{l+j-k}, \quad l+j > k \text{ 时},$$

从而 $l=k$ 时，有

$$i_j^{\pi^k} = i_{k+j-k} = i_j, \quad j = 1,2,\cdots,k.$$

显然

$$i_j^{\pi^k} = i_j, \quad j = k+1,k+2,\cdots,n.$$

所以$\pi^k=(1)$是 S_n 的单位元.

当 $1\leqslant l\leqslant k-1$ 时，

$$i_1^{\pi^l} = i_{l+1} \neq i_1 (\text{因 } l+1 \leqslant k, l \neq 0),$$

即$\pi^l\neq(1)$. 所以$|\pi|=k$.

证三 设 $\pi=(i_1\ i_2\cdots\ i_k)$是 S_n 中的一个 k-循环置换，则

$$i_1^{\pi} = i_2, \quad i_1^{\pi^2} = (i_1^{\pi})^{\pi} = i_2^{\pi} = i_3,$$
$$i_1^{\pi^3} = i_4, \quad \cdots, \quad i_1^{\pi^{k-1}} = i_k, \quad i_1^{\pi^k} = i_1.$$

类似地，有

$$i_2^{\pi^k} = i_2, \quad \cdots, \quad i_k^{\pi^k} = i_k.$$

显然

$$i_j^{\pi^k} = i_j, \quad k+1 \leqslant j \leqslant n,$$

从而 $\pi^k=(1)$是 S_n 的单位元.

当 $0<l<k$ 时，由上可知，i_1 总是被 π^l 变动，因此 $\pi^l\neq(1)$. 所以$|\pi|=k$.

证四 设 $\pi=(i_1\ i_2\cdots\ i_k)$是集 $A=\{a_1,a_2\cdots,a_n\}=\{a_{i_1},a_{i_2},\cdots,a_{i_n}\}$的一个 k-循环置换，$1\leqslant l\leqslant k$.

$\lambda<k$ 时，$a_{i_\lambda}^{\pi}=a_{i_{\lambda+1}}\Rightarrow a_{i_\lambda}^{\pi^l}=\begin{cases}a_{i_{\lambda+l}}(\lambda+l\leqslant k)\\ a_{i_{\lambda+l-k}}(\lambda+l>k)\end{cases}\Rightarrow a_{i_\lambda}^{\pi^k}=a_{i_{\lambda+k-k}}=a_{i_\lambda}$.

$\lambda=k$ 时，$a_{i_\lambda}^{\pi}=a_{i_1}\Rightarrow a_{i_\lambda}^{\pi^l}=a_{i_l}\Rightarrow a_{i_\lambda}^{\pi^k}=a_{i_\lambda}$.

$\lambda>k$ 时，$a_{i_\lambda}^{\pi}=a_{i_\lambda}\Rightarrow a_{i_\lambda}^{\pi^l}=a_{i_\lambda}\Rightarrow a_{i_\lambda}^{\pi^k}=a_{i_\lambda}$.

所以，$1\leqslant j\leqslant n$ 时，

$$a_{i_j}^{\pi^k} = a_{i_j} = a_{i_j}^{\varepsilon},$$

从而 $\pi^k=\varepsilon$ 是恒等变换.

$\forall\, s:0<s<k$，都有

$$a_{i_k}^{\pi^s} = a_{i_s} \neq a_{i_k} = a_{i_k}^{\varepsilon}.$$

即 $\pi^s\neq\varepsilon$. 所以$|\pi|=k$.

注　1)　利用该命题,直接可知$(1\ 2\ 3)^2(2\ 3\ 1)^{-1}(3\ 5\ 4\ 1)=(1\ 2\ 5\ 4)$的阶为4.

2)　我们把k-循环置换中的k叫做该循环置换的长. 于是该题可推广为如下命题:

任一置换π都可写成不相连的循环置换的乘积,则π的阶等于这些循环置换的长的最小公倍数.

证一　设$\pi=\eta_1\eta_2\cdots\eta_s$,其中$\eta_1,\eta_2,\cdots,\eta_s$是不相连的循环置换. 设$\eta_i$的长为$l_i$,则由该题知,$|\eta_i|=l_i,i=1,2,\cdots,s$. 设$|\pi|=d$,又设$l_1,l_2,\cdots,l_s$的最小公倍数是$m$,下面我们只需证明$d=m$.

因$\eta_1,\eta_2,\cdots,\eta_s$不相连,故由上面1,1)题知

$$\pi^m=(\eta_1\eta_2\cdots\eta_s)^m=\overbrace{(\eta_1\eta_2\cdots\eta_s)(\eta_1\eta_2\cdots\eta_s)\cdots(\eta_1\eta_2\cdots\eta_s)}^{m个}$$
$$=\eta_1^m\eta_2^m\cdots\eta_s^m.$$

因$l_i\mid m$,故$\exists q_i\in\mathbf{Z}$,使得$m=l_iq_i$,从而

$$\eta_i^m=\eta_i^{l_iq_i}=\left(\eta_i^{l_i}\right)^{q_i}=e^{q_i}=e,\quad i=1,2,\cdots,s.$$

所以,$\pi^m=e$,又$|\pi|=d$,于是$d\mid m$.

另一方面,因$\pi^d=\eta_1^d\eta_2^d\cdots\eta_s^d$,又$\pi^d=e$,故$\eta_1^d\eta_2^d\cdots\eta_s^d=e$. 由$\eta_1^d,\eta_2^d,\cdots,\eta_s^d$没有共同数字知,$\eta_i^d=e$. 又由$|\eta_i|=l_i$知$l_i\mid d,i=1,2,\cdots,s$,即$d$是$l_1,l_2,\cdots,l_s$的公倍数. 因$m$是$l_1,l_2,\cdots,l_s$的最小公倍数,故$m|d$. 又$m$与$d$都是正整数,所以$d=m$.

证二　设π可写成不相连的循环置换的乘积:$\pi=\eta_1\eta_2\cdots\eta_s$. 由上面题1,1)知,$\forall$整数$t$,有$\pi^t=\eta_1^t\eta_2^t\cdots\eta_s^t$. 所以$\pi^t=e\Leftrightarrow\eta_i^t=e,i=1,2,\cdots,s$. 又因$|\eta_i|=\eta_i$的长度$l_i$,故$\eta_i^t=e\Leftrightarrow l_i\mid t$. 从而,

$$\pi^t=e\Leftrightarrow l_i\mid t,i=1,2,\cdots,s.$$

设$|\pi|=d$,则$\pi^d=e\Rightarrow l_i\mid d$,即$d$是$l_1,l_2,\cdots,l_s$的公倍数. 设$k$是$l_1,l_2,\cdots,l_s$的任一公倍数,则$l_i\mid k\Rightarrow\pi^k=e\Rightarrow d\mid k$. 所以$d$是$l_1,l_2,\cdots,l_s$的最小公倍数.

证三　设π可写成不相连的循环置换的乘积.

$$\pi=(x_{11}\cdots x_{1l_1})(x_{21}\cdots x_{2l_2})\cdots(x_{s1}\cdots x_{sl_s}).$$

又设$|\pi|=d$. 下面证明d是$l_1,l_2,\cdots,l_s$的最小公倍数.

由上面1,1)题知

$$\pi^d=(x_{11}\cdots x_{1l_1})^d(x_{21}\cdots x_{2l_2})^d\cdots(x_{s1}\cdots x_{sl_s})^d.$$

因$\pi^d=\varepsilon$,故

$$(x_{11}\cdots x_{1l_1})^d(x_{21}\cdots x_{2l_2})^d\cdots(x_{s1}\cdots x_{sl_s})^d=\varepsilon.$$

又因$(x_{11}\cdots x_{1l_1})^d,(x_{21}\cdots x_{2l_2})^d,\cdots,(x_{s1}\cdots x_{sl_s})^d$没有共同数字,故

$$(x_{11}\cdots x_{1l_1})^d=\varepsilon,(x_{21}\cdots x_{2l_2})^d=\varepsilon,\cdots,(x_{s1}\cdots x_{sl_s})^d=\varepsilon.$$

由该题知$|(x_{i1}\cdots x_{il_i})|=l_i$,因此$l_i|d,i=1,2,\cdots,s$,即$d$是$l_1,l_2,\cdots,l_s$的公倍数.

若k是$l_1,l_2,\cdots,l_s$的任一公倍数,则$l_i\mid k$. 于是$\exists q_i\in\mathbf{Z}$,使得$k=l_iq_i$,从而

$$(x_{i1}\cdots x_{il_i})^k=\left((x_{i1}\cdots x_{il_i})^{l_i}\right)^{q_i}=\varepsilon^{q_i}=\varepsilon,i=1,2,\cdots,s.$$

因此

$$\pi^k = (x_{11}\cdots x_{1l_1})^k(x_{21}\cdots x_{2l_2})^k\cdots(x_{s1}\cdots x_{sl_s})^k = \varepsilon\varepsilon\cdots\varepsilon = \varepsilon.$$

今$|\pi|=d$,故$d|k$. 所以d是$l_1,l_2,\cdots,l_s$的最小公倍数.

例 置换$\pi=\begin{pmatrix}1&2&3&4&5&6&7\\4&3&2&6&7&1&5\end{pmatrix}=(1\ 4\ 6)(2\ 3)(5\ 7)$. 于是$|\pi|=3,2,2$的最小公倍数$=6$.

3. 证明:S_n的每一个元都可以写成

$$(1\ 2),(1\ 3),\cdots,(1\ n)$$

这$n-1$个2-循环置换中的若干个的乘积.

证一 已知S_n的每一个元都可以写成若干个不相连的循环置换的乘积,从而只需证明任一个k-循环置换$(i_1\ i_2\cdots\ i_k)$都可以表成$(1\ 2),(1\ 3),\cdots,(1\ n)$中的若干个的乘积.

先对k作数学归纳法,证明任一个k-循环置换都可表为一些对换的乘积:

$$(i_1\ i_2\ \cdots\ i_k) = (i_1\ i_2)(i_1\ i_3)\ \cdots\ (i_1\ i_k).$$

1) $k=1$时,$(i_1)=(i_1j)(i_1j)$.

2) 假定$k-1$时,等式成立,即

$$(i_1\ i_2\ \cdots\ i_{k-1}) = (i_1\ i_2)(i_1\ i_3)\ \cdots\ (i_1\ i_{k-1}).$$

今看k时,

$$(i_1\ i_2)(i_1\ i_3)\cdots(i_1\ i_{k-1})(i_1\ i_k)=(i_1\ i_2\cdots i_{k-1})(i_1\ i_k)$$

$$=\begin{pmatrix}i_1\ i_2\cdots i_{k-1}\ i_k i_{k+1}\cdots i_n\\ i_2\ i_3\cdots i_1\quad i_k i_{k+1}\cdots i_n\end{pmatrix}\begin{pmatrix}i_1\ i_2\cdots\ i_{k-1}\ i_k\ i_{k+1}\cdots\ i_n\\ i_k\ i_2\cdots\ i_{k-1}\ i_1\ i_{k+1}\cdots\ i_n\end{pmatrix}$$

$$=\begin{pmatrix}i_1\ i_2\cdots i_{k-1}\ i_k i_{k+1}\cdots i_n\\ i_2\ i_3\cdots i_k\quad i_1\ i_{k+1}\cdots i_n\end{pmatrix}(i_1\ i_2\cdots\ i_k).$$

由归纳原理,对于任意自然数k,有

$$(i_1\ i_2\ \cdots\ i_k) = (i_1\ i_2)(i_1\ i_3)\cdots(i_1\ i_k).$$

当$i_1=1$时,本题得证. 当$i_1\neq1$时,若$i_2,i_3,\cdots,i_k$中有某个$i_j=1$,则

$$(i_1\ \cdots\ i_{j-1}\ i_j\ i_{j+1}\ \cdots\ i_k) = (i_j\ i_{j+1}\ \cdots\ i_k\ i_1\ \cdots\ i_{j-1})$$

$$= (i_j\ i_{j+1})\cdots\ (i_j\ i_k)(i_j\ i_1)\ \cdots\ (i_j\ i_{j-1}).$$

本题也得证. 今考虑$i_l\neq1$,其中$l=1,2,\cdots,k$时,

因

$$(i_1\ i_2) = (1\ i_1)(1\ i_2)(1\ i_1),$$

$$(i_1\ i_3) = (1\ i_1)(1\ i_3)(1\ i_1),$$

$$\cdots\cdots$$

$$(i_1\ i_k) = (1\ i_1)(1\ i_k)(1\ i_1).$$

故

$$(i_1\ i_2\ \cdots\ i_k) = (i_1\ i_2)(i_1\ i_3)\ \cdots(i_1\ i_k)$$

$$=(1\ i_1)(1\ i_2)(1\ i_1)(1\ i_1)(1\ i_3)(1\ i_1)\cdots\ (1\ i_1)(1\ i_k)(1\ i_1).$$

所以本题得证.

证二 由于每一个置换π都可以写成若干个不相连的循环置换的乘积,所以只需证明,一个循环置换可以写成若干个置换$(1\ i)(i=2,3,\cdots,n)$的乘积. 可分以下两种情况.

1)　1 在置换 π 中出现，这时，

$$\pi=(1\ i_1\ i_2\cdots\ i_{k-1})=(1\ i_1)(1\ i_2)\ \cdots\ (1\ i_{k-1});$$

2)　1 不在置换 π 中出现，这时，

$$\pi=(i_1\ i_2\ \cdots\ i_k)=(1\ i_1\ i_2\ \cdots\ i_k)(1\ i_1)$$
$$=(1\ i_1)\ (1\ i_2)\ \cdots\ (1\ i_k)(1\ i_1).$$

注　1)　S_n 可以看成是由集$\{(1\ 2),(1\ 3),\cdots,(1\ n)\}$生成的群，即 $S_n=(\{(1\ 2),(1\ 3),\cdots,(1\ n)\})$.

2)　置换表示成 2-循环置换的乘积时，表法并不唯一.

例　$(1\ 2\ 3)=(1\ 2)\ (1\ 3)=(1\ 2)(1\ 3)(1\ 2)(1\ 2)$.

4. 证明：一个循环群一定是交换群.

证一　设 $G=(a)$，$\forall\, a^h, a^k\in G$，都有

$$a^h\,a^k=a^{h+k}=a^{k+h}=a^k\,a^h.$$

所以循环群是交换群.

证二　因为整数加群 $\mathbb{Z}$ 与模 n 的剩余类加群 $\mathbb{Z}_n$ 都是交换群，所以由第六章，一，4 中结论知循环群也是交换群①.

注　该命题的逆命题不成立.

例　全体实数 G 对于数的加法来说作成一个交换群，但 G 不是循环群. 不然，若 $G=(a)$，则 $\forall\, b\in G$，$\exists\, n\in\mathbb{Z}$，使得 $b=na$. 取 $1\in G$，也 $\exists\, n(\neq 0)\in\mathbb{Z}$，使得 $1=n_1a$，从而 $a=\dfrac{1}{n_1}$是有理数. 取$\sqrt{2}\in G$，$\exists\, m(\neq 0)\in\mathbb{Z}$，使得$\sqrt{2}=ma$，从而 $a=\dfrac{\sqrt{2}}{m}$是无理数，出现矛盾.

又例　非零实数集 G 对于数的乘法作成一个交换群. 假设 $G=(a)$. 因 $a^{1.5}$是非零实数，故 $a^{1.5}\in G$. $\forall\, n\in\mathbb{Z}$，由 a^x 的严格单调性知 $a^{1.5}\neq a^n$，从而 $a^{1.5}\overline{\in}(a)=G$，此为矛盾. 所以 G 不是循环群.

又例　$\mathbb{Z}[\mathrm{i}]=\{a+b\mathrm{i}\mid a,b\in\mathbb{Z}\}$关于数的加法作成交换群. 但 $\mathbb{Z}[\mathrm{i}]$不是循环加群. 事实上，假设 $\mathbb{Z}[\mathrm{i}]$是循环加群，则 $\mathbb{Z}[\mathrm{i}]=(a+b\mathrm{i})$. $\mathrm{i}\in(a+b\mathrm{i})$，从而 $\mathrm{i}=n(a+b\mathrm{i})=na+nb\mathrm{i}$，于是 $na=0$，$nb=1$，因此 $a=0$. 又 $1\in(a+b\mathrm{i})$，从而 $1=m(a+b\mathrm{i})=ma+mb\mathrm{i}$，于是 $ma=1$，$mb=0$，因此 $b=0$. 可见 $a+b\mathrm{i}=0$. 此与 $\mathbb{Z}[\mathrm{i}]=(a+b\mathrm{i})$矛盾. 所以 $\mathbb{Z}[\mathrm{i}]$不是循环加群.

5. 假定群的元 a 的阶是 n. 证明：a^r 的阶是$\dfrac{n}{d}$，这里 $d=(r,n)$是 r 和 n 的最大公因子.

证一　因$(r,n)=d$，故 $r=dr_1$，$n=dn_1$，且$(r_1,n_1)=1$，从而

$$(a^r)^{\frac{n}{d}}=(a^n)^{\frac{r}{d}}=(a^n)^{r_1}\overset{\text{由}|a|=n}{=\!=\!=}e^{r_1}=e.$$

设正整数 p 也使$(a^r)^p=e$，则 $a^{rp}=e$. 又 $|a|=n$，于是 $n\mid rp$，即 $dn_1\mid dr_1p$. 因 $d\neq 0$，故 $n_1\mid r_1p$. 又$(n_1,r_1)=1$，因此 $n_1\mid p$，即$\dfrac{n}{d}\mid p$. 因 $p>0$，故 $p\geqslant\dfrac{n}{d}$. 所以$|a^r|=\dfrac{n}{d}$.

证二　设$|a^r|=t$. 只需证 $t=\dfrac{n}{d}$，即只需证 $t\mid\dfrac{n}{d}$，同时$\dfrac{n}{d}\mid t$.

---

①　张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 21. 定理 1.

因$(r,n)=d$，故$r=dr_1$，$n=dn_1$，且$(r_1,n_1)=1$.

由

$$(a^r)^{\frac{n}{d}}=(a^n)^{\frac{r}{d}}=(a^n)^{r_1}\xlongequal{|a|=n}e^{r_1}=e.$$

又$|a^r|=t$，有$t\Big|\frac{n}{d}$.

另一方面，$(a^r)^t=a^n=e$，又$|a|=n$，从而$n\big|rt$，即$dn_1\big|dr_1t$. 因$d\neq 0$，故$n_1\big|r_1t$. 因$(r_1,n_1)=1$，故$n_1\big|t$，即$\frac{n}{d}\Big|t$.

综上，t与$\frac{n}{d}$都是正整数，因此$|a^r|=t=\frac{n}{d}$.

注 1） 该题与阶的基本概念联系紧密，证明方法有一定代表性、典型性.

2） 设$|a|=n$，又$(r,n)=1$，则$|a^r|=n$.

3） 该题的逆命题也成立. 即：设群的元a的阶是n，且$|a^r|=\frac{n}{d}$，则$d=(r,n)$是r和n的最大公因子.

证 因$|a^r|=\frac{n}{d}$，故$d\big|n$. 因$(a^r)^{\frac{n}{d}}=e$，即$a^{r\cdot\frac{n}{d}}=e$. 而$|a|=n$，故$n\Big|r\cdot\frac{n}{d}$，从而$\exists k\in\mathbb{Z}$，使得$r\cdot\frac{n}{d}=nk$，即$rn=nkd$，因$n\neq 0$，故$r=kd$，因此$d\big|r$. 所以d是r和n的公因子.

设$m=(r,n)$，则$d\big|m$. 因$(a^r)^{\frac{n}{m}}=(a^n)^{\frac{r}{m}}=e$，又$|a^r|=\frac{n}{d}$，故$\frac{n}{d}\Big|\frac{n}{m}$，从而$\exists q\in\mathbb{Z}$，使得$\frac{n}{m}=q\cdot\frac{n}{d}$，即$nd=qnm$. 又$n\neq 0$，因此$d=qm$，于是$m\big|d$. 又$d,m$都是正整数，故$d=m$. 所以$d=(r,n)$.

6. 假定a生成一个阶是n的循环群G. 证明：a^r也生成G，假如$(r,n)=1$（这就是说r和n互素）.

证一 只需证$(a)=(a^r)$. 显然$(a^r)\subset(a)$，下面证明$(a)\subset(a^r)$，也就是要证明生成元a是a^r的乘方. 由$(r,n)=1$，$\exists\lambda,\mu\in\mathbb{Z}$，使得$\lambda r+\mu n=1$. 从而$a=a^{\lambda r+\mu n}=a^{\lambda r}(a^n)^{\mu}\xlongequal{\text{由}|a|=n}(a^r)^{\lambda}e^{\mu}=(a^r)^{\lambda}$.

$\forall a^h\in(a)$，有

$$a^h=\left((a^r)^{\lambda}\right)^h=(a^r)^{\lambda h}\in(a^r).$$

因此$(a)\subset(a^r)$. 综上，有$(a^r)=(a)=G$.

证二 只需证$(a)=(a^r)$. 因$|(a)|=n$，故$|a|=n$. 由上面5题，$|a^r|=\frac{n}{(n,r)}=n$，从而$|(a^r)|=n=|(a)|$，又$(a^r)\subset(a)$，所以$(a^r)=(a)=G$.

注 1） 证二主要利用了证明两个有限集相等的一种方法，即：设G与$\overline{G}$都是有限集，若$G\subset\overline{G}$，且G与$\overline{G}$含有相同个数的元素，则$G=\overline{G}$①.

---

① 张禾瑞．近世代数基础．北京：高等教育出版社，1978. 39. 定理的证明．

2)　该命题的逆命题也成立，即：设 $G=(a)$ 的阶 $=n$，且 $G=(a^r)$，则 $(r,n)=1$.

证一　因 $|a|=|(a)|=n$，且 $|a^r|=|(a^r)|=|(a)|=n=\frac{n}{1}$，故由上面题 5，注 3)知，$(r,n)=1$.

证二　因 $a\in G=(a^r)$，故 $\exists m\in\mathbb{Z}$，使得 $a=(a^r)^m=a^{rm}$，从而 $a^{1-rm}=e$. 因 $|a|=n$，故 $n|1-rm$，于是 $\exists q\in\mathbb{Z}$，使得 $1-rm=nq$，即 $rm+nq=1$. 所以 $(r,n)=1$.

证三　设 $(r,n)=d$，则 $r=dq_1,n=dq_2$，其中 q_1,q_2 都是正整数．由

$$(a^r)^{q_2}=a^{rq_2}=a^{dq_1q_2}=a^{nq_1}=(a^n)^{q_1}=e.$$

又 $|a^r|=|(a^r)|=|(a)|=n$，从而 $n\,\big|\,q_2$. 又 $q_2\,\big|\,n$，n,q_2 都是正整数，因此 $n=q_2$，于是 $d=1$. 所以

$$(r,n)=1.$$

证四　(反证法) 若 $(r,n)\neq1$，设 $(r,n)=d>1$，则 $|a^r|=\frac{n}{d}<n$，于是 $|(a^r)|\neq n=|G|$，即 $(a^r)\neq G$，此与已知矛盾．所以 $(r,n)=1$.

例　因模 n 的剩余类加群 $\mathbb{Z}_n=([1])$ 的阶是 n，故

$$(k,n)=1\Leftrightarrow\mathbb{Z}_n=(k[1]).$$

3)　设①G 是 n 阶循环群；②u 是小于 n 且与 n 互素的正整数个数 $\phi(n)$，即 $u=\phi(n)$ [欧拉(Euler)函数]，则 G 的生成元恰有 $\phi(n)$ 个.

因为由本题，G 的生成元至少有 $\phi(n)$ 个，由注 2)，G 的生成元至多有 $\phi(n)$ 个，所以 G 的生成元有且只有 $\phi(n)$ 个.

4)　无限循环群 $G=(a)$ 有且只有两个生成元 a 与 a^{-1}.

证一　由第六章，一，4 中结论，$G\cong\mathbb{Z}$，因此，只需解决 $\mathbb{Z}$ 有且只有两个生成元.

因 $\forall k\in\mathbb{Z}$，都有 $k=(\pm k)(\pm1)$，故 ±1 是 $\mathbb{Z}$ 的两个生成元，即 $\mathbb{Z}=(1)=(-1)$.

设 a 是 $\mathbb{Z}$ 的一个生成元，则对于 $1\in\mathbb{Z}$，$\exists m\in\mathbb{Z}$，使得 $1=ma$，从而 $a|1$. 因只有 ±1 才能整除 1，故 $a=\pm1$，即 $\mathbb{Z}$ 只有两个生成元 1 与 -1.

所以，无限循环群 $G=(a)$ 的生成元也是有且只有两个，它们分别对应于 $\mathbb{Z}$ 的生成元 1 和 -1，即 a 与 a^{-1}.

证二　因为

$$\begin{aligned}G=(a)&=\left\{a^n\,\middle|\,n\in\mathbb{Z}\right\}=\{\cdots,a^{-2},a^{-1},a^0=e,a,a^2,\cdots\}\\&=\left\{\cdots,(a^{-1})^{-2},(a^{-1})^{-1},(a^{-1})^0=e,a^{-1},(a^{-1})^2,\cdots\right\}\\&=\left\{(a^{-1})^n\,\middle|\,n\in\mathbb{Z}\right\}=(a^{-1}).\end{aligned}$$

所以，a 与 a^{-1} 都是 G 的生成元.

设 b 是 G 的生成元，则 $\exists m\in\mathbb{Z}$，使得 $b^m=a$；另一方面，因 $b\in G$，故 $\exists k\in\mathbb{Z}$，使得 $b=a^k$，从而

$$a=b^m=(a^k)^m=a^{km}.$$

因 $|a|=\infty$，故 $km=1$. 所以 $k=\pm1,m=\pm1$，即 b 是 a 或 a^{-1}. 于是 G 有且只有两个生成元 a 与 a^{-1}.

有且只有两个生成元的循环群未必是无限的. 例，4 阶循环群 $\mathbb{Z}_4$ 有且只有两个生成元：[1]，[3].

例 设 ε 是一个 12 次本原单位根，则全部 12 次单位根所成的群是

$$U_{12}=(\varepsilon)=\left\{\varepsilon^k \middle| k=0,1,2,\cdots,11\right\}.$$

U_{12} 共有 $\phi(12)=4$ 个生成元：$\varepsilon,\varepsilon^5,\varepsilon^7,\varepsilon^{11}$.

7. 假定 G 是循环群，并且 G 与 $\overline{G}$ 同态. 证明：$\overline{G}$ 也是循环群.

证 $\overline{G}$ 也是一个群①. 要证明 $\overline{G}$ 是循环群，只需证明 $\overline{G}$ 有一个生成元.

因 G 是循环群，故 $G=(a)$. 设 ϕ 是 G 到 $\overline{G}$ 的同态满射，则 $\exists\,\bar{a}\in\overline{G}$，使

$$\phi: a\to\bar{a}=\phi(a).$$

$\forall\,\bar{b}\in\overline{G}$，因 ϕ 是满射，故 $\exists\,a^k\in G$，使得

$$\phi: a^k\to\bar{b}.$$

当 k 是正整数时，因 ϕ 保持运算，故

$$\phi: a^k=\overbrace{a\,a\,\cdots\,a}^{k\text{个}}\to\overbrace{\bar{a}\bar{a}\cdots\bar{a}}^{k\text{个}}=\bar{a}^k.$$

当 k 是 0 时，

$$\phi: a^k=a^0=e\to\bar{e}=\bar{a}^0=\bar{a}^k.$$

当 k 是负整数时，

$$\phi: a^k=(a^{-1})^{-k}=\overbrace{a^{-1}\,a^{-1}\cdots\,a^{-1}}^{-k\text{个}}\to\overbrace{\bar{a}^{-1}\,\bar{a}^{-1}\cdots\,\bar{a}^{-1}}^{-k\text{个}}=(\bar{a}^{-1})^{-k}=\bar{a}^k.$$

综上，

$$\phi: a^k\to\bar{a}^k.$$

因 ϕ 是映射，故 $\bar{b}=\bar{a}^k$. 所以 $\overline{G}=(\bar{a})=(\phi(a))$.

注 1) 循环群 G 到循环群 $\overline{G}$ 的同态满射把生成元映到生成元，即 G 的生成元 a 在同态满射 ϕ 下的象 $\phi(a)$ 是 $\overline{G}$ 的生成元.

2) 该命题的逆命题不成立. 即：若 $\overline{G}=(a)$，群 $G\sim\overline{G}$，但 G 未必是循环群.

例 由第六章，二，4，注，例，$\mathbb{Z}[\mathrm{i}]$ 不是循环加群. $\mathbb{Z}=(1)$ 是循环加群. 而 $\phi: a+b\mathrm{i}\to a+b$ 是 $\mathbb{Z}[\mathrm{i}]$ 到 $\mathbb{Z}$ 的一个同态满射.

又例 取 $G=S_3$，$\overline{G}=\{1,-1\}$ 对于数的乘法作成一个循环群 (-1). ϕ：(1)，$(1\ 2\ 3)$，$(1\ 3\ 2)\to 1$，$(1\ 2)$，$(1\ 3)$，$(2\ 3)\to -1$ 是 G 到 $\overline{G}$ 的一个同态满射. 但因 G 不可换，故 G 不是循环群.

该例也说明当 $\overline{G}$ 是交换群时，虽群 $G\sim\overline{G}$，但 G 未必可换.

3) 设 $G=(a)$，$\overline{G}=(\bar{a})$，$G\overset{\phi}{\sim}\overline{G}$，但 $\bar{a}$ 在 ϕ 下的逆象未必都是 G 的生成元.

例 $\mathbb{Z}=(1)$，$\mathbb{Z}_2=\{[0],[1]\}=([1])$，$\phi: a\to[a]$ 是 $\mathbb{Z}$ 到 $\mathbb{Z}_2$ 的一个同态满射. $[1]$ 在 ϕ 下的逆象有 $\pm1,\pm3,\pm5,\cdots$，其中只有 ±1 是 $\mathbb{Z}$ 的生成元.

8. 假定 G 是无限阶的循环群，$\overline{G}$ 是任何循环群，证明：G 与 $\overline{G}$ 同态.

证一 设 $G=(a)$，$\overline{G}=(\bar{a})$. 则

$$\phi: a^k\to\bar{a}^k$$

是 G 到 $\overline{G}$ 的一个同态满射. 事实上，

1) $\forall\,x\in G$，因 $|a|=\infty$，故 $\exists|\,k\in\mathbb{Z}$，使得 $x=a^k$，从而 $\exists|\,\bar{a}^k\in\overline{G}$，使得 $\phi(a^k)=\bar{a}^k$. 所以

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 40. 定理 1.

ϕ是映射.

2) $\forall y\in\overline{G}=(\bar{a})$,都$\exists k\in\mathbb{Z}$,使得$y=\bar{a}^k$,从而$\exists a^k\in G$,使得$\phi(a^k)=\bar{a}^k=y$. 所以$\phi$是满射.

3) $\forall a^k,a^h\in G$,有

$$\phi(a^ka^h)=\phi(a^{k+h})=\bar{a}^{k+h}=\bar{a}^k\bar{a}^h=\phi(a^k)\phi(a^h).$$

所以ϕ是G到$\overline{G}$的一个同态满射.

证二 1) 若$\overline{G}$是无限阶的循环群,设$G=(a)$,$\overline{G}=(\bar{a})$. 作

$$\phi:a^k\to\bar{a}^k.$$

则ϕ是G到$\overline{G}$的同态满射(实际上,ϕ还是同构映射). 事实上,

① $\forall a^k\in G$, $\exists\bar{a}^k\in\overline{G}$,使得

$$\phi:a^k\to\bar{a}^k.$$

若$a^h=a^k$,因$|a|=\infty$,故$h=k$,从而$\exists|\bar{a}^k\in\overline{G}$,使得

$$\phi:a^k\to\bar{a}^k.$$

所以ϕ是映射.

② $\forall\bar{a}^k\in\overline{G}$, $\exists a^k\in G$,使得

$$\phi:a^k\to\bar{a}^k.$$

所以ϕ是满射.

③ $\forall a^k,a^h\in G$,

$$\phi:a^k\to\bar{a}^k,\ a^h\to\bar{a}^h.$$

$$\phi:a^ka^h=a^{k+h}\to\bar{a}^{k+h}=\bar{a}^k\bar{a}^h.$$

所以ϕ是G到$\overline{G}$的一个同态满射.

2) 若$\overline{G}$是有限阶的循环群. 设$G=(a)$, $\overline{G}=(\bar{a})$,且$|\bar{a}|=n$,即$\overline{G}=\{\bar{a}^0=\bar{e},\bar{a},\bar{a}^2,\cdots,\bar{a}^{n-1}\}$. 作

$$\psi:a^k\to\bar{a}^h,\text{当且仅当}\ k=nq+h,q\in\mathbb{Z},0\leqslant h<n,$$

则ψ是G到$\overline{G}$的同态满射. 事实上,

① $\forall a^k\in G$,有$k=nq+h,q\in\mathbb{Z},0\leqslant h<n$,且这个$h$是唯一的. 又若$a^l=a^k$,由$|a|=\infty$,有$l=k$,从而$\exists|\bar{a}^h\in\overline{G}$,使得

$$\psi:\ a^k\to\bar{a}^h.$$

所以ψ是映射.

② $\forall\bar{a}^h\in\overline{G}$,作$h+nq=k$,其中$q$是任意整数,从而$\exists k\in\mathbb{Z}$,即$\exists a^k\in G$,使得

$$\psi:\ a^k\to\bar{a}^h.$$

所以ψ是满射.

③ $\forall a^{k_1},a^{k_2}\in G$,

$$\psi:\ a^{k_1}\to\bar{a}^{h_1},\text{当且仅当}\ k_1=nq_1+h_1,\ 0\leqslant h_1<n.$$

$$\psi:\ a^{k_2}\to\bar{a}^{h_2},\text{当且仅当}\ k_2=nq_2+h_2,\ 0\leqslant h_2<n.$$

于是

$$k_1+k_2=(nq_1+h_1)+(nq_2+h_2)=n(q_1+q_2)+h_1+h_2.$$

设$h_1+h_2=nq_3+h_3,0\leqslant h_3<n$,则

$$k_1+k_2=n(q_1+q_2+q_3)+h_3,\ 0\leqslant h_3<n,$$

从而

$$\psi: a^{k_1}a^{k_2}=a^{k_1+k_2}\to \bar{a}^{h_3}\xlongequal{\text{由}\ |\bar{a}|=n}\bar{a}^{h_3+nq_3}=\bar{a}^{h_1+h_2}=\bar{a}^{h_1}\bar{a}^{h_2}.$$

所以 $G\overset{\psi}{\sim}\overline{G}$.

证三 1) 若 $\overline{G}$ 是无限阶的循环群，则由第六章，一，4 中结论知 $\overline{G}$ 的生成元的阶无限，且 $\overline{G}$ 与整数加群 $\mathbb{Z}$ 同构．同理 G 也与整数加群 $\mathbb{Z}$ 同构．所以 G 与 $\overline{G}$ 同构，当然 G 与 $\overline{G}$ 同态.

2) 若 $\overline{G}$ 是有限阶的循环群，设其阶为 n，则由第六章，一，4 中结论知 $\overline{G}$ 与模 n 的剩余类加群 $\mathbb{Z}_n$ 同构，因而只需证明整数加群 $\mathbb{Z}$ 与 $\mathbb{Z}_n$ 同态. 作

$$\phi: a\to[a],$$

则 ϕ 是 $\mathbb{Z}$ 到 $\mathbb{Z}_n$ 的一个同态满射. 事实上，

① $\forall a\in\mathbb{Z}$，$\exists|[a]\in\mathbb{Z}_n$，使得

$$\phi: a\to[a].$$

所以 ϕ 是映射.

② $\forall[a]\in\mathbb{Z}_n$，$\exists a\in\mathbb{Z}$，使得

$$\phi: a\to[a].$$

所以 ϕ 是满射.

③ $\forall a,b\in\mathbb{Z}$，

$$\phi: a\to[a], b\to[b].$$

且

$$\phi: a+b\to[a+b]=[a]+[b].$$

所以 $\mathbb{Z}\overset{\phi}{\sim}\mathbb{Z}_n$，即 $G\sim\overline{G}$.

证四 1) 若 $\overline{G}$ 是无限阶的循环群，见证二.

2) 若 $\overline{G}$ 是有限阶的循环群，由第六章，一，4 中结论知 $\overline{G}$ 与模 n 的剩余类加群 $\mathbb{Z}_n$ 同构，因此，只需证 $G=(a)\sim\mathbb{Z}_n$. 设

$$\phi: a^k\to[k].$$

① $\forall a^k\in G$，$\exists[k]\in\mathbb{Z}_n$，使得

$$\phi: a^k\to[k].$$

若 $a^h=a^k$，因 $|a|=\infty$，故 $h=k$，从而 $\exists|[k]\in\mathbb{Z}_n$，使

$$\phi: a^k\to[k].$$

所以 ϕ 是映射.

② $\forall[k]\in\mathbb{Z}_n$，$\exists a^k\in G$，使得

$$\phi: a^k\to[k].$$

所以 ϕ 是满射.

③ $\forall a^h,a^k\in G$，

$$\phi: a^h\to[h],\ a^k\to[k].$$

且

$$\phi: a^h a^k=a^{h+k}\to[h+k]=[h]+[k].$$

所以 $G\overset{\phi}{\sim}\mathbb{Z}_n$，又 $\mathbb{Z}_n\sim\overline{G}$，于是 $G\sim\overline{G}$.

注 设 G 是无限阶的循环群，$\overline{G}$ 是任何循环群，那么 $\overline{G}$ 与 G 未必同态.

若 $\overline{G}$ 是无限阶的循环群，则显然 $\overline{G}$ 与 G 同态. 若 $\overline{G}$ 是有限阶的循环群，不妨设 $\overline{G}=\mathbb{Z}_n$，$G=\mathbb{Z}$. 因 $\overline{\exists}$ $\mathbb{Z}_n$ 到 $\mathbb{Z}$ 的满射，故 $\mathbb{Z}_n$ 到 $\mathbb{Z}$ 不同态，即 $\overline{G}$ 与 G 不同态.

读者可考虑 $\phi:[a]\rightarrow a$ 是否为 $\mathbb{Z}_n$ 到 $\mathbb{Z}$ 的满射.

三、讲与练

1. 证明：n 元集 A 的每一个 n 元置换 π，如果不计因子次序及 1-循环置换的取舍，那么 π 可唯一地写成若干个不相连的循环置换的乘积.

证一　若 π 是恒等置换，命题显然成立. 若 π 不是恒等置换，则无论怎样把 π 分解成若干个不相连的循环置换的乘积，其中都必有一个循环置换含 i_1，且 $\pi(i_1)=i_2$，且 $i_2\neq i_1$. 继续下去，$\pi(i_2)=i_3,\cdots,\pi(i_k)=i_1$，于是这个循环置换就是 $(i_1\ i_2\cdots\ i_k)$. 而且由于 π 是一一映射，这个含 i_1 的循环置换是且只能是 $(i_1\ i_2\cdots\ i_k)$，出现在 π 的每一种分解式中. 若还 $\exists j_1$，且 $j_1\neq i_l$，$l=1,2,\cdots,k$，同理含 j_1 的循环置换 $(j_1\ j_2\cdots\ j_k)$ 必然出现在 π 的每一种分解式中. 如此类推，得知在 π 的各种分解式中，含任一数字的循环置换都是相同的. 因为 A 是有限集，所以在 π 的各种分解为不相连的循环置换的乘积的分解式中，只有可能出现循环置换因子次序的不同（由第六章，二，1 知，两个不相连的循环置换可以交换），或 1－循环置换是否写入的不同，从而分解式唯一.

证二　对被 π 变动的元的个数 l 作数学归纳法.

1)　$l=0$ 时，$\pi=(1)$ 是恒等置换，命题显然成立.

2)　假定被变动的元的个数少于 $l(\geqslant 1)$ 的 n 元置换分解成不相连的循环置换的乘积的分解式是唯一的，今看变动 $l(\geqslant 1)$ 个元的 n 元置换 π. 因 $l\geqslant 1$，故必 $\exists i_1$，而 $\pi(i_1)=i_2$，$i_2\neq i_1$，继续下去，由 π 是一一映射，A 是有限集，必经有限步，得 $\pi(i_2)=i_3,\cdots,\pi(i_k)=i_1$，即

$$\pi=(i_1\ i_2\cdots i_k)\pi_1.$$

其中 π_1 是一个被变动的元的个数少于 l 的 n 元置换. 由归纳假设，π_1 可以唯一地写成若干个不相连的循环置换的乘积，所以 π 也同样可以写成了.

据归纳原理，命题得证.

2. 利用 Cayley 定理，

1)　写出与 Klein 四元群 $B_4=\{a,b,c,d\}$ 同构的置换群. B_4 的运算表如下.

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

2)　写出与模 4 的剩余类加群 $\mathbb{Z}_4$ 同构的置换群.

3)　写出与 n 阶循环群 $G=(a)$ 同构的置换群 $\overline{G}$. 由此可以说明什么问题？

解　1)

$$\begin{array}{llll} \tau_a: & a\to aa=a & \tau_b: & a\to ab=b \\ & b\to ba=b & & b\to bb=a \\ & c\to ca=c & & c\to cb=d \\ & d\to da=d, & & d\to db=c, \\ \tau_c: & a\to ac=c & \tau_d: & a\to ad=d \\ & b\to bc=d & & b\to bd=c \\ & c\to cc=a & & c\to cd=b \\ & d\to dc=b, & & d\to dd=a \end{array}$$

是 B_4 的 4 个变换．为了书写简明起见，把 B_4 中的元 a, b, c, d 依次记为 1,2,3,4．于是

$$\tau_a=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=(1),\qquad \tau_b=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=(1\ 2)(3\ 4),$$

$$\tau_c=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=(1\ 3)(2\ 4),\qquad \tau_d=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}=(1\ 4)(2\ 3).$$

由 Cayley 定理，B_4 与置换群$\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$同构．

2） $\mathbb{Z}_4=\{[0],[1],[2],[3]\}$．

$$\tau_{[0]}:[a]\to[a]+[0]=[a],\qquad \tau_{[1]}:[a]\to[a]+[1]=[a+1],$$
$$\tau_{[2]}:[a]\to[a]+[2]=[a+2],\quad \tau_{[3]}:[a]\to[a]+[3]=[a+3].$$

如果 $\mathbb{Z}_4$ 的 4 个元素$[0],[1],[2],[3]$依次用数码 1,2,3,4 来代表的话，那么有

$$\tau_{[0]}=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=(1),\qquad \tau_{[1]}\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}=(1\ 2\ 3\ 4),$$

$$\tau_{[2]}\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=(1\ 3)(2\ 4),\qquad \tau_{[3]}\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}=(1\ 4\ 3\ 2).$$

作置换群

$$\overline{G}=\{(1),(1\ 2\ 3\ 4),(1\ 3)(2\ 4),(1\ 4\ 3\ 2)\}=\big((1\ 2\ 3\ 4)\big).$$

由 Cayley 定理，$\phi:[a]\to\tau_{[a]}$是 $\mathbb{Z}_4$ 与 $\overline{G}$ 间的一个同构映射，即 $\mathbb{Z}_4\cong\overline{G}$.

3） 因 $G\cong\overline{G}$，而 $G=(a)$是 n 阶循环群，故 $\overline{G}$ 也是 n 阶循环群，且 $\overline{G}$ 的生成元是 G 的生成元 a 在同构映射下的象．由 Cayley 定理的证明知 a 的象是 τ_a，而 $\tau_a:x\to xa$，于是有

$$\tau_a=\begin{Bmatrix}e & a & a^2 & \cdots & a^{n-1}\\ a & a^2 & a^3 & \cdots & e\end{Bmatrix}=\begin{pmatrix}1&2&3&\cdots&n\\2&3&4&\cdots&1\end{pmatrix}=(1\ 2\ 3\ \cdots\ n).$$

所以 $\overline{G}=\big((1\ 2\ 3\ \cdots\ n)\big)$.

由此可说明任意有限阶的置换群都存在．比如 3 阶置换群为$\big((1\ 2\ 3)\big)$，它与模 3 的剩余类加群 $\mathbb{Z}_3$同构．又比如 6 阶置换群为$((1\ 2\ 3\ 4\ 5\ 6))$，它与模 6 的剩余类加群 $\mathbb{Z}_6$同构．

3. 证明：n 次单位根乘群 $U_n=\{z\mid z\text{ 是复数},z^n=1\}$是一个循环群．

证

$$U_n=\left\{\varepsilon_k\,\middle|\,\varepsilon_k=\cos\frac{2k\pi}{n}+\mathrm{i}\sin\frac{2k\pi}{n},\ k=0,1,2,\cdots,n-1\right\}.$$

$\forall\,\varepsilon_k\in U_n$，

$$\varepsilon_k = \cos\frac{2k\pi}{n} + \mathrm{i}\sin\frac{2k\pi}{n} = e^{\frac{2k\pi}{n}\cdot \mathrm{i}} = \left(e^{\frac{2\pi}{n}\cdot \mathrm{i}}\right)^k$$
$$= \left(\cos\frac{2\pi}{n} + \mathrm{i}\sin\frac{2\pi}{n}\right)^k = \varepsilon_1^k,$$

从而 ε_1 是 U_n 的一个生成元，$U_n=(\varepsilon_1)$是一个 n 阶循环群.

注　取任一 n 次本原单位根 ε_1^l，$(l,n)=1$，则 ε_1^l 也是 U_n的一个生成元，即 $U_n=(\varepsilon_1^l)$.

4. 设 $G=(a)$是无限循环群，证明：G 中任一元素 $b(\neq e)$的阶都无限.

证一　设 G 中有一元素 $c(\neq e)$的阶有限，且 $|c|=n(\neq 0)$，则 $c^n=e$. 又 $c\in G=(a)$，从而 $c=a^m$，即 $e=c^n=(a^m)^n=a^{mn}$. 因 $|a|=\infty$，故 $mn=0$，即 $m=0$，$c=a^m=e$，发生了矛盾. 所以 G 中任一元素 $b(\neq e)$的阶都无限.

证二　因 $G=(a)$是无限循环群，故ϕ：$a^k\to k$ 是 G 与整数加群 $\mathbb{Z}$ 间的一个同构映射[①]. $\forall b=a^m\in G$，ϕ：$b=a^m\to m$. 其中 $b\neq e$，从而 $m\neq 0$.

$$(b) = \left\{b^s \middle| s\in\mathbb{Z}\right\} = \left\{a^{ms} \middle| s\in\mathbb{Z}\right\}.$$

若 $t\neq s$，而 $b^t=b^s$，则 $a^{mt}=a^{ms}$. 因 $m\neq 0$，故 $mt\neq ms$，此与ϕ是映射矛盾. 所以 $b^t\neq b^s$，即(b)无限，从而$|b|$无限.

5. 设 k 与 n 是两个整数，证明：

$$k\,\big|\,n \Leftrightarrow (k)\supset(n),$$

其中(k)，(n)是循环加群.

证　($\Rightarrow$)　因 $k\,|\,n$，故 $\exists\, q\in\mathbb{Z}$，使得 $n=kq$. $\forall\, np\in(n)$，$np=(kq)p=k(qp)\in(k)$. 从而$(n)\subset(k)$.

($\Rightarrow$)　$n\in(n)$，又$(n)\subset(k)$，于是 $n\in(k)$，即 $\exists\, l\in\mathbb{Z}$，使得 $n=kl$，从而 $k\,|\,n$.

6. 设 a,b 是任二整数，证明：

1)　$(a)\cap(b)=(c)$，其中 c 是 a,b 的最小公倍数，(a)，(b)，(c)是循环加群.

2)　记$\left\{au+bv \middle| u,v\in\mathbb{Z}\right\}$为$(a)+(b)$，则$(a)+(b)=(d)$，其中 $d=(a,b)$，(a)，(b)，(d)是循环加群.

证　1)　因 $a\,|\,c$，$b\,|\,c$，由上题知$(c)\subset(a)$，$(c)\subset(b)$，故$(c)\subset(a)\cap(b)$.

另一方面，$\forall\, x\in(a)\cap(b)$，即 $x\in(a)$，$x\in(b)$，从而 $a\,|\,x$，$b\,|\,x$，即 x 是 a,b 的公倍数. 因 c 是 a,b 的最小公倍数，故 $c\,|\,x$. 于是 $x\in(c)$，从而$(a)\cap(b)\subset(c)$.

所以$(a)\cap(b)=(c)$.

2)　因$(a,b)=d$，故 $\exists\, p,q\in\mathbb{Z}$，使得 $ap+bq=d$，从而 $d\in(a)+(b)$，即$(d)\subset(a)+(b)$.

另一方面，$\forall\, x\in(a)+(b)$，即 $x=au+bv$，$u,v\in\mathbb{Z}$. 因 $d=(a,b)$，故 $d\,|\,au+bv=x$，从而 $x\in(d)$，即$(a)+(b)\subset(d)$.

所以$(a)+(b)=(d)$.

---

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 59. 定理的证明.

四、思考问题

1. 计算.

1) $(1\ 2\ 4\ 6\ 5\ 7)^{-2}=?$

2) 方程$(1\ 2\ 4)x=(3\ 4\ 6)(1\ 5)$的解是什么?

3) 方程$(i\ j)x=(i\ k)$的解是什么?

2. 下面命题成立否:设$a,b,c,d\in$群G,且$|a|=|b|$,$|c|=|d|$,则$|ac|=|bd|$.

3. 设$H=\{1,-1\}$对于实数的普通乘法作成一个群. 证明:三次对称群$S_3=\{(1),(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2)\}$与$H$同态.

4. 设p是素数,问S_p内有多少个p阶元?

5. 下面各命题对否.

1) 一个循环群除单位元外,每个元都生成它.

2) 循环群的每个元都生成一个循环群.

3) 一切阶相同的循环群都是同构的.

4) 恰有16个互不同构的、阶不大于16的循环群.

5) 一个循环群的阶不能是n^2,如果n不是奇数.

6) 若一个群含有一个无限阶元素,则这个群必是循环群.

7) 因由ab生成的循环群是交换群,故$ab=ba$.

8) 所有形如$\begin{pmatrix}1 & 0\\ n & 1\end{pmatrix}$($n$是整数)的方阵的集对于方阵的乘法作成一个循环群.

9) S_3是一个循环群.

10) $G=\{2^n \mid n\in\mathbb{Z}\}$对于普通乘法作成一个循环群.

11) $G=\{[0],[2],[4],[6]\}$对于模8的剩余类加法作成一个循环群.

12) 设$a,b\in$群G,n是整数,若$a^n=b^n$,则$a=b$.

6. 证明:

1) 设$G_1=(a)$与$G_2=(b)$是两个无限循环群,则有且只有两个G_1与G_2间的同构映射.

2) 设$G_1=(a)$与$G_2=(b)$是两个n阶循环群,则有且只有$\varphi(n)$个G_1与G_2间的同构映射,这里$\varphi(n)$是欧拉函数,表示小于n且与n互素的正整数的个数.

7. 求出模6的剩余类加群$\mathbb{Z}_6$的每一个元的阶,并求出$\mathbb{Z}_6$的所有生成元.

8. 设(a)是一个s阶循环群,(b)是一个t阶循环群,k是一个固定的正整数,证明:

$$t\mid sk \Leftrightarrow \text{存在一个}(a)\text{到}(b)\text{的同态映射}\phi: a\to b^k, e\to e',$$

其中e,e'分别是(a),(b)的单位元.

第七章　子群、子群的陪集

一、基本问题问答

1. 给出一个例子：G 与 H 都是群，且 H 是 G 的子集，但 H 不是 G 的子群.

答　例，G 是整数加群，$H=\{0,1\}$ 对于

	0	1
0	0	1
1	1	0

作成一个群，且 $H\subset G$，但 H 不是 G 的子群. 因为 H 对于 G 的代数运算：普通加法，不作成一个群.

又如 G 是有理数加群，H 是全体非零有理数对于普通乘法作成的群，$H\subset G$，但 H 不是 G 的子群.

2. 设 H 是群 G 的子群，又 $H\neq\{e\}$，$H\neq G$，则称 H 是 G 的真子群. 证明：

1)　设 $G=(a)$ 是无限循环群，则 G 必有真子群.

2)　无限循环群的真子群仍是无限循环群.

3)　无限循环群与其无限真子群同构.

证　1)　因 $G=(a)$ 无限，故 $\exists a^k\in G$，且 $a^k\neq e, a^k\neq a, a^k\neq a^{-1}$，$(a^k)=H<G$. 因无限阶循环群 $G=(a)$ 的生成元有且只有两个：a 与 a^{-1}，故 $H\neq G$. 因 $a^k\neq e$，故 $H\neq\{e\}$. 从而 $H=(a^k)$ 是 G 的真子群.

2)　由第六章，三，4 知，无限循环群中除单位元外，其他的任意元的阶都无限. 所以无限循环群的真子群仍是无限循环群.

3)　因为无限循环群的真子群都是无限循环群，而任意两个无限循环群都同构，所以命题得证.

例　整数加群 $\mathbb{Z}$ 与其真子群 $n\mathbb{Z}=\left\{nk \,\middle|\, k\in\mathbb{Z}\right\}$（$n$ 是 $\neq 1$ 的正整数）同构. 由此还可见，$\mathbb{Z}$ 有无穷多个无限真子群.

3. 设 $S\subset$ 群 G，$S\neq\varnothing$，由 S 生成的子群 H 的定义是什么？利用 H 是包含 S 的 G 的最小子群，还可将 H 如何表示？

答　由 S 生成的子群 H 的定义是

$$H=(S)=\left\{a_1^{k_1}a_2^{k_2}\cdots a_n^{k_n} \,\middle|\, a_i\in S, k_i=\pm 1, n\text{ 是任意正整数}\right\}$$

$$=\left\{x_1x_2\cdots x_n \,\middle|\, x_i\in S\cup S^{-1}, n\text{ 是任意正整数}\right\},$$

其中 $S^{-1}=\left\{s^{-1}\mid s\in S\right\}$.

利用 H 是包含 S 的 G 的最小子群，还可将 H 如下表示：

$$H=(S)=\bigcap\left\{T\mid T<G,T\supset S\right\}=\bigcap_{\substack{T\supset S\\T<G}}T.$$

由此可构造 G 的子群.

当 $S<G$ 时，$(S)=S$.

4. 设 H 是群 G 的子群，Ha 是 H 的含 $a(\in G)$ 的右陪集，证明：

1) $a\in H\Leftrightarrow Ha=H$.

2) $Ha<G\Leftrightarrow Ha=H$.

证 1) $(\Rightarrow)$ $\forall h\in H$，因 $a\in H$，H 是群，故 $h=(ha^{-1})a\in Ha$，从而 $H\subset Ha$.

另一方面，$\forall ha\in Ha$，因 $h,a\in H$，H 是群，故 $ha\in H$，从而 $Ha\subset H$.

综上，$Ha=H$.

$(\Leftarrow)$ 因 $a=ea\in Ha$，又 $Ha=H$，故 $a\in H$.

2) $(\Rightarrow)$ 因 $Ha<G$，故 $e\in Ha$，又 $e\in He$，从而 $Ha=He=H$.

$(\Leftarrow)$ 因 $Ha=H$，$H<G$，故 $Ha<G$.

注 在群 G 的子群 H 的右陪集中，有且只有一个右陪集 $Ha=H(a\in H)$ 是 G 的子群. 其他的 H 的右陪集 $Hx(x\overline{\in}H)$ 都不是 G 的子群.

5. 在命题“一个子群 H 的右陪集的个数和左陪集的个数相等”的证明中，若规定

$$\phi:Ha\to aH,$$

那么 ϕ 是否为 $S_r=\left\{Ha\mid a\in G\right\}$ 到 $S_l=\left\{aH\mid a\in G\right\}$ 的一个映射？

答 不是. 因为 $Ha=Hb$ 时，未必 $aH=bH$，即 $Ha(\in S_r)$ 在 ϕ 下的象 aH 不一定唯一，而是受代表 a 的选择的影响.

例 $H=\{(1),(1\ 2)\}$ 是 S_3 的子群. $H(1\ 3)=H(1\ 2\ 3)$，但 $(1\ 3)H\neq(1\ 2\ 3)H$. 因 $(1\ 2\ 3)^{-1}(1\ 3)=(3\ 2\ 1)(1\ 3)=(2\ 3)\overline{\in}H$.

6. 证明：对于群 G 的任意子群 H 来说，一个左陪集中的元素的逆元组成一个右陪集.

证 取定 $a\in G$，只需证 $\left\{(ah)^{-1}\mid h\in H\right\}=Ha^{-1}$.

$$\forall (ah)^{-1}\in\left\{(ah)^{-1}\mid h\in H\right\},(ah)^{-1}=h^{-1}a^{-1}\in Ha^{-1}.$$

$$\forall ha^{-1}\in Ha^{-1},ha^{-1}=(ah^{-1})^{-1}\in\left\{(ah)^{-1}\mid h\in H\right\}.$$

所以 $\left\{(ah)^{-1}\mid h\in H\right\}=Ha^{-1}$，即左陪集 aH 中的元素的逆元组成一个右陪集.

7. 1) 子群 $\{e\}$ 在群 G 里的指数是什么？

2) 子群 G 在群 G 里的指数是什么？

答 1) $\forall a,b\in G,a\neq b$，则含 a 与含 b 的 $\{e\}$ 的左陪集

$$a\{e\}=\{ae\}\neq\{be\}=b\{e\}.$$

即 $a\{e\}$ 与 $b\{e\}$ 是各含一个元的不同的集. 因此子群 $\{e\}$ 在群 G 里的指数是 G 中所含元的个数.

2) $\forall a\in G$，含 a 的 G 的左陪集

$$aG=\left\{ag\mid g\in G\right\}=G.$$

因此子群 G 在群 G 里的指数是 1.

注 将子群 H 在群 G 里的指数记为 $[G:H]$，从而 $[G:\{e\}]=G$ 中所含元的个数．$[G:G]=1$.

8. 1) 怎样的群有且只有一个子群？

2) 怎样的群有且只有两个子群？

答 1) 群 $\{e\}$ 有且只有一个子群 $\{e\}$.

2) 素数阶群 G 有且只有两个子群 $\{e\}$ 及 G. 因为素数 p 阶群 G 的子群的阶必为 p 的因子：1 与 p. 所以 G 的子群有且只有 $\{e\}$ 及 G.

9. 证明：一个阶为 mn(m,n 是正整数)的循环群有阶为 m 和阶为 n 的元素.

证 设 $G=(a)$，且 $|G|=mn$，从而 $|a|=mn$，于是 $a^{mn}=(a^m)^n=(a^n)^m=e$. $\forall l: 0<l<n$，$(a^m)^l=a^{ml}\neq e$（因 $0<ml<mn$，又 $|a|=mn$），所以 $|a^m|=n$. 同理 $|a^n|=m\left(利用第六章，二，5 亦可知 |a^m|=\frac{mn}{(mn,m)}=\frac{mn}{m}=n\right)$.

10. 设 G 是有限循环群，$\forall$ 正整数 m，$m\,\big|\,|G|$，则 G 有 m 阶元，从而 G 有 m 阶子群.

证 因 $m\,|\,|G|$，故 $|G|=ms$，$s\in\mathbb{Z}$. 设 $G=(a)$，由上题知 $|a^s|=m$. 且 G 有 m 阶子群 (a^s).

注 Lagrange 定理[①]的逆命题："设 G 是有限群. 若正整数 m，$m\,\big|\,|G|$，则 G 有 m 阶子群"不成立．但当 G 是有限循环群时，Lagrange 定理的逆命题成立.

二、典型问题分析

1. 找出 S_3 的所有子群.

解一 $H_1=S_3$，$H_2=\{(1)\}$，$H_3=\{(1),(1\ 2)\}$，$H_4=\{(1),(1\ 3)\}$，$H_5=\{(1),(2\ 3)\}$，$H_6=\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$ 是 S_3 的子群[②].

S_3 仅有以上 6 个子群. 因为

(i) $(ij)(ik)=(ijk)$.

(ii) $(ijk)^2=(ikj)$.

(iii) $(ij)(ijk)=(ik)$.

(iv) $(ij)(ikj)=(jk)$.

从而

1) 只含(1)及两个或三个 2-循环置换的集合不是子群(由(i)知).

2) 只含(1)及一个 3-循环置换的集合不是子群(由(ii)知).

3) 只含(1)及两个 3-循环置换和一个 2-循环置换的集合不是子群(由(iii)知).

4) 只含(1)及两个 3-循环置换和两个 2-循环置换的集合不是子群(由(iii)，(iv)知).

所以 S_3 有且仅有以上 6 个子群.

解二 H_1,H_2,H_3,H_4,H_5,H_6 是 S_3 的 6 个子群(见解一). 若子群 H' 不是以上的 5 个

---

① 张禾瑞．近世代数基础．北京：高等教育出版社，1978. 69. 定理 2.

② 同上．63. 定理 3.

子群：H_2, H_3, H_4, H_5, H_6. 那么

1) 或 H'至少含有两个 2-循环置换，比如(ij)，(ik). 此时$(ij)(ik)=(ijk)\in H'$，$(ijk)(ij)=(jk)\in H'$，$(ij)(jk)=(ikj)\in H'$，$(ij)(ij)=(i)\in H'$，从而 $H'=H_1=S_3$.

2) 或 H'至少含有一个 2-循环置换和一个 3-循环置换，比如(ij)和(ijk). 此时$(ijk)^2=(ikj)\in H'$，$(ij)(ijk)=(ik)\in H'$，$(ij)(ikj)=(jk)\in H'$，$(ij)(ij)=(i)\in H'$，从而 $H'=H_1=S_3$.

所以上面给出的 6 个子群是 S_3 的所有的子群.

注 此题说明，若群 G 的所有真子群都可换(是循环群)，但 G 未必可换(是循环群).

2. 证明：群 G 的两个子群的交集也是 G 的子群.

证 设 H_1, H_2 是群 G 的两个子群. 因 $e\in H_1, e\in H_2$，故 $e\in H_1\cap H_2$，从而 $H_1\cap H_2\neq\varnothing$. 显然 $H_1\cap H_2\subset G$. $\forall a,b\in H_1\cap H_2$，有 $a,b\in H_1$，且 $a,b\in H_2$. 因 H_1, H_2 都是 G 的子群，故 $ab^{-1}\in H_1$，且 $ab^{-1}\in H_2$，从而 $ab^{-1}\in H_1\cap H_2$. 于是 $H_1\cap H_2<G$①.

注 1) 设 H_1, H_2 是群 G 的两个子群，但 H_1 与 H_2 的并集 $H_1\cup H_2$ 未必是 G 的一个子群.

例 $H_1=\{2k\mid k\in\mathbb{Z}\}$，$H_2=\{3l\mid l\in\mathbb{Z}\}$是整数加群 $\mathbb{Z}$ 的两个子群，则

$$H_1\cup H_2=\{2k,3l\mid k,l\in\mathbb{Z}\}.$$

$2,3,\in H_1\cup H_2$，但 $2+3=5$ 既不是 $2k$ 形状，又不是 $3l$ 形状，故 $2+3\,\overline{\in}\, H_1\cup H_2$，从而 $H_1\cup H_2$对加法不封闭. 所以 $H_1\cup H_2$ 不是 $\mathbb{Z}$ 的子群.

又例 $H_1=\{(1),(1\ 2)\}<S_3$，$H_2=\{(1),(1\ 3)\}<S_3$，但 $H_1\cup H_2=\{(1),(1\ 2),(1\ 3)\}$不是 S_3 的子群，因$(1\ 2)(1\ 3)=(1\ 2\ 3)\,\overline{\in}\, H_1\cup H_2$.

2) 设 $H_1<G, H_2<G$，则

$$H_1\cup H_2<G\Leftrightarrow H_1<H_2 \text{ 或 } H_2<H_1.$$

证一 ($\Leftarrow$) $H_1<H_2$ 时，$H_1\cup H_2=H_2<G$；$H_2<H_1$ 时，$H_1\cup H_2=H_1<G$.

($\Rightarrow$) (反证法) 若 H_1 不是 H_2 的子群，而且 H_2 也不是 H_1 的子群，则 $\exists a\in H_1$，但 $a\,\overline{\in}\, H_2$，$\exists b\in H_2$，但 $b\,\overline{\in}\, H_1$，于是 $ab\,\overline{\in}\, H_1\cup H_2$. 事实上，若 $ab\in H_1\cup H_2$，则 $ab\in H_1$ 或 $ab\in H_2$. 当 $ab=h_1\in H_1$ 时，$b=a^{-1}h_1\in H_1$，此与 $b\,\overline{\in}\, H_1$ 矛盾. 当 $ab=h_2\in H_2$ 时，$a=h_2b^{-1}\in H_2$，此与 $a\,\overline{\in}\, H_2$ 矛盾. 所以 $ab\,\overline{\in}\, H_1\cup H_2$，但 $a\in H_1\cup H_2$，$b\in H_1\cup H_2$，故 $H_1\cup H_2$ 对乘法不封闭. 此与已知条件 $H_1\cup H_2<G$ 矛盾. 所以，$H_1<H_2$ 或 $H_2<H_1$.

证二 若 $H_1<H_2$，则命题成立. 若 H_1 不是 H_2 的子群，则 $\exists a\in H_1$，但 $a\,\overline{\in}\, H_2$. $\forall b\in H_2$，则 $a,b\in H_1\cup H_2$. 又 $H_1\cup H_2<G$，从而 $ab\in H_1\cup H_2$，于是 $ab\in H_1$ 或 $ab\in H_2$. 由 $a\in H_1$，但$a\,\overline{\in}\, H_2$知，$ab=c\,\overline{\in}\, H_2$(否则，若 $ab=c\in H_2$，则 $a=cb^{-1}\in H_2$，矛盾). 所以只能 $ab=d\in H_1$，因此 $b=a^{-1}d\in H_1$. 这说明 $H_2\subset H_1$，又 $H_1<G, H_2<G$，所以 $H_2<H_1$.

3. 证明：循环群的子群也是循环群.

证一 设 $G=(a)$，$H<G$.

当 $H=\{e\}$时，$H=(e)$是循环群.

当 $H\neq\{e\}$时，$\exists a^k\in H$，$a^k\neq e$，而 $k>0$(不然，若 $k=0$，$a^k=e$，矛盾. 若 $k<0$，则$(a^k)^{-1}=$

① 张禾瑞．近世代数基础．北京：高等教育出版社，1978. 63. 定理 2.

$a^{-k}\in H$，此时$-k>0$）. 则集 $P=\{k\,|\,a^k\in H, k>0\}\neq\varnothing$，$P$ 中有最小正整数 k_0，使 $a^{k_0}\in H$，则$H=(a^{k_0})$. 事实上，$\forall b\in H$，因 $H\subset G=(a)$，故 $b=a^t$. 设 $t=k_0q+r, q\in\mathbb{Z}, 0\leqslant r<k_0, r=t-k_0q$，于是

$$a^r=a^{t-k_0q}=a^t(a^{k_0})^{-q}=b(a^{k_0})^{-q}.$$

因 $b, a^{k_0}\in H$，又 H 是群，故 $a^r\in H$. 又 $0\leqslant r<k_0$，由 k_0 是 P 中的最小正整数，得 $r=0$，从而 $t=k_0q$，即 $b=(a^{k_0})^q$. 所以 $H=(a^{k_0})$是循环群.

证二　如证一，$H<G=(a)$，k_0 是集 P 中的最小正整数，则 $a^{k_0}\in H$，从而$(a^{k_0})\subset H$.

$\forall b\in H\subset G=(a)$，都有 $b=a^t$，且 $k_0\,|\,t$. 事实上，假设不然，若$\exists a^l\in H, l\neq 0$，但 $k_0\nmid l$. 设$(k_0,l)=d, d>0$，则因 $k_0\nmid l$，故 $d<k_0$. 此时$\exists$整数 u,v，使 $k_0u+lv=d$. 于是

$$a^d=a^{k_0u+lv}=(a^{k_0})^u(a^l)^v\in H,$$

从而 $d\in P$. 但 $d<k_0$，此与 k_0 是 P 中的最小正整数矛盾．因此$\forall b\in H$，都有 $b=a^t$，且 $k_0\,|\,t$，即$\exists q\in\mathbb{Z}$，使得 $t=k_0q$，从而 $b=a^{k_0q}=(a^{k_0})^q\in(a^{k_0})$. 所以 $H=(a^{k_0})$.

注　1)　对该命题，下面证法不对：

设 $G=(a)$，$H<G$. $\forall x\in H$，则 $x\in G$，因此 x 就可以写成 a 的乘方，从而由定义，H 是循环群.

因为 a 未必属于 H.

2)　该命题的逆命题不对. 即：一个群如果除本身外所有子群都是循环群，这个群本身未必是循环群．例，Klein 4 元群 $B_4=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$，它的子群除本身外都是 1 阶和 2 阶的，从而都是循环群，但 B_4 不是循环群，因为在 B_4 中没有 4 阶元.

又例，设 $G=\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\pm\begin{pmatrix}i&0\\0&-i\end{pmatrix},\pm\begin{pmatrix}0&1\\-1&0\end{pmatrix},\pm\begin{pmatrix}0&i\\i&0\end{pmatrix}\right\}$，其中 $i^2=-1$. 则 G 对于矩阵乘法作成一个非交换群，且 G 的每个子群除本身外都是循环群. 事实上，令

$$e=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad a_1=\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\ a_2=\begin{pmatrix}i&0\\0&-i\end{pmatrix},\ a_3=\begin{pmatrix}-i&0\\0&i\end{pmatrix},$$

$$a_4=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\ a_5=\begin{pmatrix}0&-1\\1&0\end{pmatrix},\ a_6=\begin{pmatrix}0&i\\i&0\end{pmatrix},\ a_7=\begin{pmatrix}0&-i\\-i&0\end{pmatrix}.$$

G 的乘法表为

	e	a_1	a_2	a_3	a_4	a_5	a_6	a_7
e	e	a_1	a_2	a_3	a_4	a_5	a_6	a_7
a_1	a_1	e	a_3	a_2	a_5	a_4	a_7	a_6
a_2	a_2	a_3	a_1	e	a_6	a_7	a_5	a_4
a_3	a_3	a_2	e	a_1	a_7	a_6	a_4	a_5
a_4	a_4	a_5	a_7	a_6	a_1	e	a_2	a_3
a_5	a_5	a_4	a_6	a_7	e	a_1	a_3	a_2
a_6	a_6	a_7	a_4	a_5	a_3	a_2	a_1	e
a_7	a_7	a_6	a_5	a_4	a_2	a_3	e	a_1

由乘法表知 G 对于矩阵乘法封闭. 矩阵乘法当然适合结合律. G 中每一元都在表的各

行、各列出现且只出现一次，因此 G 的乘法适合消去律．所以 G 是一个群，称 G 为 4 元数群．由表易见 G 不是交换群．

因 $|G|=8$，由 lagrange 定理知，G 的子群的阶只能是 1,2,4,8．而 2 阶子群必为循环群，只能由阶为 2 的元生成，但 G 中阶为 2 的元只有一个 a_1，从而 2 阶子群只有一个为：$H_1=\{e,a_1\}=(a_1)$．G 中除 e,a_1 外其余各元的阶都是 4，从而 G 的 4 阶子群都是循环群，共有 3 个：

$$H_2=(a_2)=(a_3)=\{e,a_1,a_2,a_3\},$$
$$H_3=(a_4)=(a_5)=\{e,a_1,a_4,a_5\},$$
$$H_4=(a_6)=(a_7)=\{e,a_1,a_6,a_7\}.$$

所以 G 除本身外所有子群都是循环群．但因 G 是非交换群，故 G 不是循环群．

4. 找出模 12 的剩余类加群的所有子群．

解一 $\mathbb{Z}_{12}=\{[0],[1],[2],\cdots,[11]\}=([1])$ 是循环群，由上题知，$\mathbb{Z}_{12}$ 的子群都是循环群．因 $\mathbb{Z}_{12}$ 有 12 个元，故 $\mathbb{Z}_{12}$ 最多有 12 个子群，但这 12 个子群中可能有重复的．下面我们具体找出 $\mathbb{Z}_{12}$ 的所有的不同的子群．

1) $H_1=([0])=\{[0]\}$.

2) $H_2=([1])=\mathbb{Z}_{12}$.

因 $|\mathbb{Z}_{12}|=12$，又 $(5,12)=(7,12)=(11,12)=1$，故由第六章，二，6 知 $H_2=([5])=([7])=([11])$.

3) $H_3=([2])=\{[0],[2],[4],[6],[8],[10]\}$.

因 $|H_3|=6$，又 $(5,6)=1$，故 $H_3=(5[2])=([10])$.

4) $H_4=([3])=\{[0],[3],[6],[9]\}$.

因 $|H_4|=4$，又 $(3,4)=1$，故 $H_4=(3[3])=([9])$.

5) $H_5=([4])=\{[0],[4],[8]\}$.

因 $|H_5|=3$，又 $(2,3)=1$，故 $H_5=(2[4])=([8])$.

6) $H_6=([6])=\{[0],[6]\}$.

以上 6 个子群 $H_1,H_2,\cdots,H_6$ 就是 $\mathbb{Z}_{12}$ 的所有的子群．

解二 $\mathbb{Z}_{12}=([1])$ 是 12 阶循环群，由第六章，二，6，$\mathbb{Z}_{12}$ 的子群都是循环群，由 Lagrange 定理及第七章，一，10 知，子群的阶必是且只能是 1,2,3,4,6,12．因此 $\mathbb{Z}_{12}$ 的所有子群是：

1) $H_1=([0])$ 是 1 阶子群．

2) $H_2=([1])$ 是 12 阶子群．

3) 因 $|2[1]|=\dfrac{12}{(12,2)}=6$，故 $H_3=([2])$ 是 6 阶子群．

4) 因 $|3[1]|=\dfrac{12}{(12,3)}=4$，故 $H_4=([3])$ 是 4 阶子群．

5) 因 $|4[1]|=\dfrac{12}{(12,4)}=3$，故 $H_5=([4])$ 是 3 阶子群．

6) 因 $|6[1]|=\dfrac{12}{(12,6)}=2$，故 $H_6=([6])$ 是 2 阶子群．

因为循环群的各阶子群分别都是唯一确定的（见第七章，三，2，1)），所以 $\mathbb{Z}_{12}$ 的所有子群

是：$H_1, H_2, \cdots, H_6$.

5. 假定 H 是群 G 的一个非空子集，并且 H 的每一个元的阶都有限. 证明：H 作成子群的充要条件是

$$a, b \in H \Rightarrow ab \in H.$$

证　(⇒)　由 H 是 G 的子群的定义即知，$\forall a, b \in H$，有 $ab \in H$.

(⇐)　已知 $\varnothing \neq H \subset G$，$\forall a, b \in H$，有 $ab \in H$. $\forall\ a \in H$，下面证明 $a^{-1} \in H$. 因 $|a|$ 有限，故可设 $|a| = m$，m 是正整数，即 $a^m = e$，从而 $aa^{m-1} = e$. 于是 $a^{-1} = a^{m-1}$. 当 $m-1 > 0$ 时，由已知条件 $a^{-1} = a^{m-1} = \overbrace{a\,a\ \cdots\ a}^{(m-1)个} \in H$；当 $m-1=0$ 时，$|a| = m = 1$，从而 $a = e$. 因此 $a^{-1} = a^{m-1} = a^0 = e = a \in H$. 所以 $H < G$.

6. 证明：阶是素数的群一定是循环群.

证　设群 G 的阶是素数 p，因 $p \geqslant 2$，故 $\exists\, a \in G$，而 $a \neq e$，即 $|a| \neq 1$. 且 $|a|\ \big|\ p$①. 但 p 是素数，$|a| \neq 1$，从而 $|a| = p$，即 $|(a)| = p$. 又 $|G| = p$，且 $(a) \subset G$，所以 $G = (a)$.

注　1)　设 $|G| =$ 素数 p，因 $(1,p) = (2,p) = \cdots = (p-1,p) = 1$，故小于 p 且与 p 互素的正整数的个数 $\phi(p) = p-1$，所以素数 p 阶循环群 G 有 $\phi(p) = p-1$ 个生成元，即 $G = (a) = (a^2) = \cdots = (a^{p-1})$，其中 $a \in G, a \neq e$. 从而素数 p 阶循环群中除单位元 e 外，其余 $p-1$ 个元都是 G 的生成元.

2)　该命题的逆命题不成立．即循环群未必是素数阶的. 例如循环群 $\mathbb{Z}_4 = ([1])$ 是 4 阶群.

7. 证明：阶是 p^m 的群（p 是素数）一定包含一个阶是 p 的子群.

证一　设群 G 的阶 $= p^m$，p 是素数，m 是正整数. 因 $p^m \geqslant 2$，故 $\exists\, a \in G$，而 $a \neq e$，即 $|a| \neq 1$，且 $|a|\ \big|\ p^m$，从而 $|a| = p^r$，$0 < r \leqslant m$. 由第六章，二，5，$|a^{p^{r-1}}| = \dfrac{|a|}{(|a|, p^{r-1})} = \dfrac{p^r}{p^{r-1}} = p$. 由第六章，一，4 中结论知，$(a^{p^{r-1}})$ 是 p 阶群，又 $(a^{p^{r-1}}) \subset G$，，所以 $(a^{p^{r-1}})$ 是 G 的 p 阶子群.

证二　在证一中，对于 $|a^{p^{r-1}}| = p$ 也可直接利用定义来证明：因为 $(a^{p^{r-1}})^p = a^{p^{r-1}\cdot p} = a^{p^r} = e$. 对于任意正整数 t，$0 < t < p$，$(a^{p^{r-1}})^t \neq e$. 不然，若 $(a^{p^{r-1}})^t = e$，即 $a^{tp^{r-1}} = e$，其中 $0 < tp^{r-1} < p^r$，此与 $|a| = p^r$ 矛盾. 所以 $|a^{p^{r-1}}| = p$.

证三　证一中 $|a^{p^{r-1}}| = p$ 的证明还可采用如下方法. 显然 $(a^{p^{r-1}})^p = e$，于是 $|a^{p^{r-1}}|$ 整除 p. 因 P 是素数，故 $|a^{p^{r-1}}| = 1$ 或 $|a^{p^{r-1}}| = p$. 若 $|a^{p^{r-1}}| = 1$，则 $a^{p^{r-1}} = e$，其中 $0 < p^{r-1} < p^r$，此与 $|a| = p^r$ 矛盾. 所以 $|a^{p^{r-1}}| = p$.

8. 假定 a 和 b 是一个群 G 的两个元，并且 $ab = ba$. 又假定 a 的阶是 m，b 的阶是 n，并且 $(m,n) = 1$. 证明：ab 的阶是 mn.

证一　由 $ab = ba$，有

$$\begin{aligned}(ab)^{mn} &= \overbrace{(ab)(ab)\cdots(ab)}^{mn个} = \overbrace{(a\,a\cdots a)}^{mn个}\ \overbrace{(b\,b\ \cdots\ b)}^{mn个} = a^{mn}b^{mn} \\ &= (a^m)^n(b^n)^m = e^n e^m = e.\end{aligned}$$

设 $(ab)^s = e$，则

$$a^{ns} = a^{ns}e^s = a^{ns}(b^n)^s = a^{ns}b^{ns} = \big((ab)^s\big)^n = e^n = e.$$

---

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 69. 定理 3.

因$|a|=m$,故$m\,|\,ns$. 又$(m,n)=1$,从而$m\,|\,s$.

$$b^{ms}=e^sb^{ms}=(a^m)^sb^{ms}=a^{ms}b^{ms}=\left((ab)^s\right)^m=e^m=e.$$

因$|b|=n$,故$n\,|\,ms$. 又$(m,n)=1$,从而$n\,|\,s$. 再由$(m,n)=1$,有$mn\,|\,s$,从而$s=0$或$s\geqslant mn$. 所以$|ab|=mn$.

证二 设$|ab|=t$,只需证$t=mn$,$t\,|\,mn$且$mn\,|\,t$. 由证一,$(ab)^{mn}=e$,从而$t\,|\,mn$. 令$H=(ab)$. 由第六章,一,4中结论,$|H|=|(ab)|=t$.

$$b^m=eb^m\overset{\text{由}|a|=m}{=\!=\!=\!=}a^mb^m\overset{\text{由}ab=ba}{=\!=\!=\!=}(ab)^m\in H.$$

因$|b|=n$,由第六章,二,5,$|b^m|=\dfrac{n}{(n,m)}=n$,从而$n|t$. 同理,

$$a^n=a^ne\overset{\text{由}|b|=n}{=\!=\!=\!=}a^nb^n\overset{\text{由}ab=ba}{=\!=\!=\!=}(ab)^n\in H.$$

因$|a|=m$,由第六章,二,5,$|a^n|=\dfrac{m}{(m,n)}=m$,从而$m\,|\,t$. 因$(m,n)=1$,故$mn\,|\,t$,已知$t|mn$,又$mn>0$,$t>0$,所以$|ab|=t=mn$.

证三 设$|ab|=t$,只需证$t\,|\,mn$且$mn\,|\,t$. 由证一,$(ab)^{mn}=e$,于是$t\,|\,mn$. 由证一,$a^{nt}=e$,因$|a|=m$,故$m\,|\,nt$,又$(m,n)=1$,从而$m\,|\,t$. 由证一,$b^{mt}=e$,因$|b|=n$,故$n\,|\,mt$,又$(m,n)=1$,从而$n\,|\,t$. 再由$(m,n)=1$,$mn\,|\,t$, 又$t|mn$,$t>0$,$mn>0$,所以$t=mn$,即$|ab|=t=mn$.

证四 由证一,$(ab)^{mn}=e$. 假设存在正整数$s<mn$,使$(ab)^s=e$,由证一,$n\,|\,s$. 因此,∃正整数q,使得$s=nq<mn$,从而$0<q<m$.

$$e=(ab)^s=(ab)^{nq}\overset{\text{由}ab=ba}{=\!=\!=\!=}a^{nq}b^{nq}\overset{\text{由}|b|=n}{=\!=\!=\!=}a^{nq}.$$

因$|a|=m$,故$m\,|\,nq$,又$(m,n)=1$,从而$m\,|\,q$,此与$0<q<m$矛盾. 于是∀正整数$k<mn$,都有$(ab)^k\neq e$,所以$|ab|=mn$.

证五 设$|ab|=t$,只需证$t\,|\,mn$且$mn\,|\,t$. 由证一,$(ab)^{mn}=e$,于是$t\,|\,mn$. 由$|a|=m$,$|a^n|=\dfrac{m}{(m,n)}=m$,从而$(ab)^n\overset{\text{由}ab=ba}{=\!=\!=\!=}a^nb^n\overset{\text{由}|b|=n}{=\!=\!=\!=}a^n$的阶为$m$,即$\left|\left((ab)^n\right)\right|=m$. 因$\left((ab)^n\right)\subset(ab)$,故$\left((ab)^n\right)$是$(ab)$的子群. 又$|(ab)|=t$,由Lagrange定理,$m\,|\,t$. 同理,$n\,|\,t$. 因$(m,n)=1$,故$mn\,|\,t$. 已知$t\,|\,mn$,且$t>0$,$mn>0$,所以$|ab|=t=mn$.

注 1) 若去掉条件$ab=ba$,该命题不成立. 即:设$a,b\in$群G,$|a|=m$,$|b|=n$,$(m,n)=1$,但未必有$|ab|=|a|\,|b|$. 例,$(1\ 2)$,$(1\ 2\ 3)\in S_3$,$|(1\ 2)|=2$,$|(1\ 2\ 3)|=3$,$(2,3)=1$, 但$(1\ 2)(1\ 2\ 3)=(1\ 3)\neq(2\ 3)=(1\ 2\ 3)(1\ 2)$. 有$|(1\ 2)(1\ 2\ 3)|=|(1\ 3)|=2\neq2\times3=|(1\ 2)|\cdot|(1\ 2\ 3)|$.

2) 该命题的逆命题成立. 即:若$c\in$群G,$|c|=mn$,且$(m,n)=1$,则分别存在唯一的a与b,使$c=ab=ba$且$|a|=m$,$|b|=n$.

证 因$(m,n)=1$,故∃整数p,q,使得$pm+qn=1$, 从而$c=c^{pm+qn}=c^{pm}\cdot c^{qn}$. 令$a=c^{qn}$,$b=c^{pm}$,因此$c=ab=ba$.

下面证明$|a|$,$|b|$分别为m,n.

$$a^m = (c^{qn})^m = (c^{nm})^q \xlongequal{\text{由}|c|=mn} e,$$
$$b^n = (c^{pm})^n = (c^{mn})^p \xlongequal{\text{由}|c|=mn} e,$$

从而$|a|\,\big|\,m$，$|b|\,\big|\,n$. 于是分别存在正整数q_1和q_2，使$m=q_1\cdot|a|$，$n=q_2\cdot|b|$. 所以$|a|\cdot|b|\,|\,mn$. 另一方面，因$ab=ba$，故$c^{|a|\cdot|b|}=(ab)^{|a|\cdot|b|}=(a^{|a|})^{|b|}(b^{|b|})^{|a|}=e\cdot e=e$. 又$|c|=mn$，从而$mn\,|\,|a|\cdot|b|$. 又$mn>0$，$|a|\cdot|b|>0$，所以$mn=|a|\cdot|b|$. 又$mn=q_1q_2\,|a|\cdot|b|$，因此$q_1q_2|a|\cdot|b|=|a|\cdot|b|$. 又$|a|\cdot|b|>0$，于是$q_1q_2=1$. 但$q_1$与$q_2$都是正整数，从而$q_1=q_2=1$. 所以$|a|=m$，$|b|=n$.

最后证明表达式$c=ab=ba$唯一. 若c有另一个表达式$c=a_1b_1=b_1a_1$，$|a_1|=m$，$|b_1|=n$. 则$ab=a_1b_1$，即$a_1^{-1}a=b_1b^{-1}$. 因

$$cb_1=b_1a_1b_1=b_1c,\ a_1c=a_1b_1a_1=ca,$$

故a_1，b_1与c都可换．又a，b是c的方幂，从而a，b分别与a_1，b_1都可换，即

$$aa_1=a_1a,\ bb_1=b_1b.$$

于是

$$a_1^{-1}a=aa_1^{-1},\ b_1b^{-1}=b^{-1}b_1,$$

即a_1^{-1}与a，b_1与b^{-1}也可换.

因$(m,n)=1$，故$\exists$整数p，q，使得$mp+nq=1$，从而

$$a_1^{-1}a = (a_1^{-1}a)^{mp+nq} = (a_1^{-1}a)^{mp}(a_1^{-1}a)^{nq} = \Big((a_1^{-1}a)^m\Big)^p\Big((b_1b^{-1})^n\Big)^q$$
$$\xlongequal[\text{由}b_1b^{-1}=b^{-1}b_1]{\text{由}a_1^{-1}a=aa_1^{-1}} \Big((a_1^{-1})^m a^m\Big)^p\Big(b_1^n(b^{-1})^n\Big)^q = e^pe^q = e,$$

且$b_1b^{-1}=a_1^{-1}a=e$，于是$a_1=a$，$b_1=b$.

还可如下证明$|a|=m$，$|b|=n$. 已知

$$a^m = e,\ b^n = e.$$

若$\exists$正整数k，$k<m$，使得$a^k=e$，即$(c^{qn})^k=e$，从而$(c^n)^{qk}=e$. 又$|c^n|=\dfrac{mn}{(mn,n)}=m$，于是$m\,\big|\,qk$. 由$pm+qn=1$，$(m,q)=1$，因此$m\,\big|\,k$，此与$0<k<m$矛盾. 所以$|a|=m$. 同理$|b|=n$.

在证明表达式$c=ab=ba$唯一时，已证$a_1^{-1}a=aa_1^{-1}$，$b_1b^{-1}=b^{-1}b_1$，$a_1^{-1}a=b_1b^{-1}$，还可如下证明$a_1=a$，$b_1=b$. 因

$$(a_1^{-1}a)^m \xlongequal{\text{由}a_1^{-1}a=aa_1^{-1}} (a_1^{-1})^m a^m = ee = e,$$
$$(b_1b^{-1})^n \xlongequal{\text{由}b_1b^{-1}=b^{-1}b_1} b_1^n(b^{-1})^n = ee = e.$$

故$|a_1^{-1}a|\,\big|\,m$，$|b_1b^{-1}|\,\big|\,n$. 又$a_1^{-1}a=b_1b^{-1}$，所以$|a_1^{-1}a|\,\big|\,(m,n)=1$，从而$|a_1^{-1}a|=1$，于是$a_1^{-1}a=e$. 所以$a_1=a$. 同理$b_1=b$.

对于表达式$c=ab=ba$唯一性的证明还可采用下面方法：若$c=a_1b_1=b_1a_1$，$|a_1|=m$，$|b_1|=n$. 则

$$a_1^n = a_1^nb_1^n \xlongequal{\text{由}a_1b_1=b_1a_1} (a_1b_1)^n = (ab)^n \xlongequal{\text{由}ab=ba} a^nb^n = a^n.$$

已知$mp+nq=1$，从而

$$a_1 = a_1^{mp+nq} = (a_1^m)^p(a_1^n)^q = e^pa^{nq} = a^{1-mp} = a(a^m)^{-p} = ae^{-p} = a.$$

又 $c=a_1b_1=ab$，今已知 $a_1=a$，由消去律，$b_1=b$.

3） 设 $a_1,a_2,\cdots,a_s\in$群 G，其阶分别为 $n_1,n_2,\cdots,n_s$，$i\neq j$ 时，$(n_i,n_j)=1$，且 $a_ia_j=a_ja_i$ $(i,j=1,2,\cdots,s)$，则 $|a_1a_2\cdots a_s|=n_1n_2\cdots n_s$.

反之，若群 G 中的元 c 的阶为 $n_1n_2\cdots n_s$. $i\neq j$ 时，$(n_i,n_j)=1$，则分别存在唯一的 $a_1,a_2,\cdots,a_s$，使 $c=a_1a_2\cdots a_s$，且 $a_ia_j=a_ja_i$，$|a_i|=n_i(i,j=1,2,\cdots,s)$.

证略.

4） 条件 $(m,n)=1$ 去掉后，该命题不成立. 即：设 $a,b\in$群 G，$ab=ba$，$|a|=m$，$|b|=n$，未必有 $|ab|=|a||b|$. 例，$[2],[3]\in \mathbf{Z}_4=\{[0],[1],[2],[3]\}$，$[2]+[3]=[3]+[2]$，$|[2]|=2$，$|[3]|=4$. $(2,4)\neq 1$. $|[2]+[3]|=|[5]|=|[1]|=4\neq 2+4=|[2]|+|[3]|$.

5） 去掉条件 $(m,n)=1$ 后，一般来说，有：若 $a,b\in$群 G，$ab=ba$，$|a|=m$，$|b|=n$，则 $|ab|$ 是 m,n 的最小公倍数 $[m,n]$ 的因数. 而且群 G 中含有阶为 $[m,n]$ 的元.

证 设 $[m,n]=s$，则 $s=mq_1$，$s=nq_2$，从而

$$(ab)^s=\overbrace{(ab)(ab)\cdots(ab)}^{s\text{个}}\overset{\text{由}ab=ba}{=\!=\!=}\overbrace{aa\cdots a}^{s\text{个}}\overbrace{bb\cdots b}^{s\text{个}}=a^sb^s$$
$$=a^{mq_1}b^{nq_2}=(a^m)^{q_1}(b^n)^{q_2}=e^{q_1}e^{q_2}=e.$$

所以 $|ab|\,\big|\,s=[m,n]$.

假设 $m=p_1^{t_1}p_2^{t_2}$，$n=p_1^{s_1}p_2^{s_2}$，且设 $t_1\geqslant s_1$，$t_2\leqslant s_2$，p_1,p_2 为不相同的素数，即 $(p_1,p_2)=1$. 则 $[m,n]=p_1^{t_1}p_2^{s_2}$. 但由 $|a|=m$，$|a^{p_2^{t_2}}|=\dfrac{m}{(m,p_2^{t_2})}=p_1^{t_1}$. 由 $|b|=n$，$|b^{p_1^{s_1}}|=\dfrac{n}{(n,p_1^{s_1})}=p_2^{s_2}$，且 $(p_1^{t_1},p_2^{s_2})=1$，故由该命题，$|a^{p_2^{t_2}}b^{p_1^{s_1}}|=p_1^{t_1}p_2^{s_2}=[m,n]$.

若 $m=p_1^{t_1}p_2^{t_2}\cdots p_k^{t_k}$，$n=p_1^{s_1}p_2^{s_2}\cdots p_r^{s_r}$，则用同样方法可证.

当 $ab\neq ba$ 时，命题不成立. 例，设 G 是实数域上所有 3 阶可逆方阵对于矩阵乘法作成的群. 取 $a=\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}$，$b=\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}\in G$，于是 $ab\neq ba$. 因 $a\neq e$，$b\neq e$，$ab\neq e$，$a^2=b^2=e$，$(ab)^2\neq e$，$(ab)^3=e$，故 $|a|=|b|=2$，$|ab|=3$，$[2,2]=2$，因此 $|ab|=3\nmid 2=[2,2]$.

虽 $a,b\in$群 G，$ab=ba$，$|a|=m$，$|b|=n$，但 $|ab|$ 未必是 $[m,n]$. 例，$\varepsilon_1=\dfrac{-1+\sqrt{3}\,\mathrm{i}}{2}$，$\varepsilon_2=\dfrac{-1-\sqrt{3}\,\mathrm{i}}{2}\in U_3=\{1,\varepsilon_1,\varepsilon_2\}$，$\varepsilon_1\varepsilon_2=\varepsilon_2\varepsilon_1$，$|\varepsilon_1|=3$，$|\varepsilon_2|=3$，而 $|\varepsilon_1\varepsilon_2|=1\neq 3=[3,3]$.

9. 假定 $\sim$ 是一个群 G 的元间的一个等价关系，并且对于 G 的任意三个元 a,x,x' 来说

$$ax\sim ax'\Rightarrow x\sim x'.$$

证明：与 G 的单位元 e 等价的元所作成的集合是 G 的一个子群.

证一 设 H 为与 G 的单位元 e 等价的元所作成的集合，即 $H=\{a\in G\,|\,a\sim e\}$. 因 $\sim$ 是一个等价关系，故 $e\sim e$，即 $e\in H$，于是 $H\neq\varnothing$，且 $H\subset G$. $\forall a,b\in H$，只需证 $ab^{-1}\in H$，即上需证 $ab^{-1}\sim e$.

因 $a,b\in H$，故 $a\sim e$，$b\sim e$，即 $ae\sim aa^{-1}$，$be\sim bb^{-1}$. 由已知条件，$e\sim a^{-1}$，$e\sim b^{-1}$，因 $\sim$ 是等价关系，故 $b^{-1}\sim a^{-1}$，即 $a^{-1}ab^{-1}\sim a^{-1}e$. 再由已知条件，$ab^{-1}\sim e$，于是 $ab^{-1}\in H$. 所以 $H<G$.

证二　由证一知：$\varnothing \neq H \subset G$.

$\forall a \in H, a \sim e$，即 $ae \sim aa^{-1}$，由已知条件，$e \sim a^{-1}$. 又 $\sim$ 是等价关系，$a^{-1} \sim e$，于是 $a^{-1} \in H$.

$\forall a, b \in H, b \sim e, a \sim e$，即 $a^{-1}ab \sim a^{-1}ae$. 由已知条件，$ab \sim a$，又 $a \sim e$，由推移律，$ab \sim e$，于是 $ab \in H$.

所以，$H < G$①.

注　1)　要证 $H < G$，必须首先明确指出有一个元$\in H$，从而 $H \neq \varnothing$. 同时指出$H \subset G$.

2)　本题证明技巧主要在于灵活运用单位元的性质. 要掌握这个方法的实质，举一反三，有利于发展思维能力.

10. 我们直接下右陪集 Ha 的定义如下：Ha 刚好包含 G 的可以写成

$$ha \ (h \in H)$$

形式的元. 由这个定义推出以下事实：G 的每一个元属于而且只属于一个右陪集.

证　取定 $a \in G$，$Ha = \{ha \mid h \in H\}$.

$\forall x \in G$，因 $H < G$，故 G 的单位元 $e \in H$，从而 $x = ex \in Hx$. 所以 G 的每一个元都属于一个右陪集.

若 $x \in G$，$x \in Ha$，又 $x \in Hb$，则 $x = h_1 a = h_2 b$，$h_1, h_2 \in H$，从而 $a = h_1^{-1} h_2 b$，$b = h_2^{-1} h_1 a$. $\forall ha \in Ha$，$ha = h(h_1^{-1} h_2 b) = (hh_1^{-1} h_2) b \in Hb$，于是 $Ha \subset Hb$；另一方面，$\forall hb \in Hb$，$hb = h(h_2^{-1} h_1 a) = (hh_2^{-1} h_1) a \in Ha$，于是 $Hb \subset Ha$. 所以 $Ha = Hb$. 因此 G 中每一个元只属于一个右陪集.

注　"由 $x \in Ha$ 得 $x \sim a$"是不对的. 因为这里 Ha 不是用等价关系 $\sim$ 来定义的类. 本题恰恰是要证明 $Ha = \{ha \mid h \in H\}$ 是 G 的一个类.

11. 证明：若我们把同构的群看作一样的，一共只存在两个阶是 4 的群. 它们都是交换群.

证　4 阶群的元的阶只可能是 1,2,4.

1)　若 4 阶群 G_1 有一个元 a 的阶为 4，则 $G_1 = (a)$ 是循环群. 由第六章，二，4，G_1 是交换群. 任意两个 4 阶循环群，由第六章，一，4 中结论知必同构. 如模 4 的剩余类加群 $\mathbb{Z}_4 = ([1]) = \{[0],[1],[2],[3]\}$，4 次单位根乘群 $U_4 = (\mathrm{i}) = \{1, -\mathrm{i}, -1, \mathrm{i}\}$ 都与 G_1 同构.

2)　若 4 阶群 $G_2 = \{e, x, y, z\}$ 没有阶为 4 的元，又 G_2 必有且只有一个阶为 1 的单位元 e，因此 G_2 必有 3 个阶为 2 的元. 由第四章，二，4，G_2 是交换群，其乘法表为

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

任意两个由阶为 1，2，2，2 的 4 个元作成的群必同构. 如 Klein 四元群 $B_4 = \{(1),$

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 62. 定理 1.

(1 2)(3 4),(1 3)(2 4),(1 4)(2 3)},群$\{t,-\frac{1}{t},-t,\frac{1}{t}\}$(其代数运算为把第二个因子代入第一个因子中的$t$)都与$G_2$同构.

$G_1=(a)$是循环群,$G_2=\{e,x,y,z\}$不是循环群,由第六章,二,7,G_1与G_2不同构.

所以在同构意义下,存在两个阶是4的群,而且它们都是交换群.

注 还可用反证法如下证明:$G_1=(a)$与$G_2=\{e,x,y,z\}$不同构. 事实上,若$\exists G_1$与G_2间的同构映射ϕ. 设$\phi:a^0\to e,a\to x$,则$\phi:a^2\to x^2=e$(因$|x|=2$). 但$a^0\neq a^2$,于是e在ϕ下的逆象不唯一,此与ϕ是单射矛盾. 所以G_1与G_2不同构.

12. 利用上题证明:一个有限非交换群至少有6个元.

证 1阶群$\{e\}$显然是交换群. 因2,3,5是素数,故由第七章,二,6,2,3,5阶群是循环群,从而由第六章,二,4,它们是交换群. 由上题,4阶群是交换群. 又已知6阶群S_3是非交换群. 所以有限非交换群的阶至少是6.

三、讲与练

1. 试判断下列各命题是否正确.

1) 若S是群G的非空子集,且$\exists x_0\in S$,使得$\forall x\in S$,都有$x_0x=xx_0=x$,即x_0是S的单位元,则x_0是G的单位元.

2) 设$H_i<$群$G,i=1,2,3$. 则

① $H_1\cup H_2=H_1\cup H_3\Rightarrow H_2=H_3$.

② $H_1\cap H_2=H_1\cap H_3\Rightarrow H_2=H_3$.

3) 正有理数集$\mathbb{Q}^+$对于普通乘法作成一个群. 正整数集$\mathbb{Z}^+$是$\mathbb{Q}^+$的不空子集,且$\forall a,b\in\mathbb{Z}^+$,都有$ab\in\mathbb{Z}^+$,则$\mathbb{Z}^+<\mathbb{Q}^+$.

4) 任何一个非单位元群都是由它的一个真子集生成.

5) 阶数相同而互不同构的有限群只有有限个.

6) 集{(1 2),(1 3)}生成群S_3.

7) 设$a\in$群$G,|G|=n$,则$a^n=e,e$是G的单位元.

8) 若一个群可由含两个元的集生成,则这个群不能是循环群.

9) 一个无限群的有限子群必有无限多个不同的右陪集.

10) 设$H<G,K<G$,若$\exists x,y\in G$,使得$xH=yK$,则$H=K$.

11) 设$H<G,K<G$,且$H\subset K$,则$[G:H]\geqslant[G:K]$.

解 1) 不正确. 例,设$\mathbb{Q}$是有理数加群,$\mathbb{Q}^+$是正有理数集,则$\varnothing\neq\mathbb{Q}^+\subset\mathbb{Q}$. $\exists 1\in\mathbb{Q}^+$,使得$\forall x\in\mathbb{Q}^+$,都有$1x=x1=x$,但1不是$\mathbb{Q}$的单位元. 0才是$\mathbb{Q}$的单位元.

2) ① 不正确. 例,取$G=S_3,H_1=S_3,H_2=\{(1)\},H_3=\{(1),(1\ 2)\}$. 显然$H_1\cup H_2=S_3=H_1\cup H_3$,但$H_2\neq H_3$.

② 不正确. 例,取$G=S_3,H_1=\{(1),(1\ 2)\},H_2=\{(1),(1\ 3)\},H_3=\{(1),(2\ 3)\}$. 显然,$H_1\cap H_2=H_1\cap H_3=\{(1)\}$,但$H_2\neq H_3$.

3) 不正确. 因取$2\in\mathbb{Z}^+$,但$2^{-1}=\frac{1}{2}\overline{\in}\mathbb{Z}^+$.

4)　正确．事实上，任何一个非单位元群都是其中所有非单位元的元所作成的真子集生成.

5)　正确．事实上，由 Cayley 定理，n 阶有限群同构于 n 元集的一个 n 阶置换群．因此只需考察互不同构的 n 阶置换群有多少个．因为任一 n 阶置换群都是 n 次对称群 S_n 的一个子群，而有限群 S_n 的子群只有有限个，所以 n 阶置换群只有有限个，从而互不同构的 n 阶置换群，即互不同构的 n 阶有限群也只有有限个.

6)　正确.

7)　正确．事实上，$|a|\,\big|\,n$，从而 $\exists q\in\mathbb{Z}$，使得 $n=|a|q$. 于是 $a^n=a^{|a|q}=(a^{|a|})^q=e^q=e$.

8)　不正确．例，群$(\{(1),(1\ 2)\})=\{(1),(1\ 2)\}=\big((1\ 2)\big)$是循环群.

9)　正确. 事实上，全体右陪集是该无限群的一个分类，而每个右陪集都是有限集，从而必有无限多个右陪集.

10)　正确. 事实上，由已知，$\exists x,y\in G$，使得 $xH=yK$. 因 G 是群，故 $\exists x^{-1}\in G$，使得 $x^{-1}xH=x^{-1}yK$，即 $H=x^{-1}yK$. 因 $H<G$，故 $e\in H=x^{-1}yK$. 从而，$eK=x^{-1}yK$，即 $K=x^{-1}yK=H$.

11)　正确. 由指数定义即可知.

2. 证明：

1)　设 $G=(a)$是 n 阶循环群，m 是正整数，$m\,\big|\,n$，则存在且只存在一个阶为 m 的 G 的子群. 因此 G 的子群的个数等于 n 的正因子的个数.

2)　设 $G=(a)$是无限循环群，$H=(a^k)<G$，而 $H\neq\{e\}$，k 是正整数，则指数$[G:H]$有限且$[G:H]=k$.

证一　1)　在第七章，一，10 中已证明存在性. 下面证明唯一性.

已知 G 有 m 阶子群(a^s)，且 $n=ms$.

设 H 是 G 的任一阶为 m 的子群，由循环群的子群仍是循环群，从而 $H=(a^t)$且$|a^t|=m$.

若 $t=s$，则 $H=(a^s)$.

若 $t\neq s$，则 $t=sq+r$，$0\leqslant r<s$.

$$e=(a^t)^m=a^{tm}=a^{(sq+r)m}=(a^{sm})^q a^{rm}=e^q a^{rm}=a^{rm}.$$

又 $0\leqslant rm<sm=n$，而$|a|=n$，于是 $rm=0$. 又 $m>0$，从而 $r=0$. 所以 $t=sq$. 因此 $a^t=a^{sq}=(a^s)^q\in(a^s)$，即 $H\subset(a^s)$. 因$|H|=|(a^s)|=m$，故 $H=(a^s)$.

所以 G 只有一个阶为 m 的 G 的子群(a^s).

2)　$\forall a^l\in G$，因 $k\neq0$，故 $\exists u,v\in\mathbb{Z}$，使得 $l=uk+v$，$0\leqslant v<k$，从而 $a^l=a^{uk+v}=(a^k)^u a^v\in Ha^v$，所以

$$G=Ha^0\cup Ha\cup Ha^2\cup\cdots\cup Ha^{k-1}(a^0=e).$$

下面证明，$Ha^i\cap Ha^j=\varnothing$，其中 $0\leqslant i,j\leqslant k-1$，$i\neq j$. 事实上，若 $Ha^i\cap Ha^j\neq\varnothing$，则 $\exists b\in Ha^i\cap Ha^j$. 于是 $b=ha^i=h'a^j$，$h,h'\in H$. 不妨设 $i>j$，则 $a^{i-j}=h^{-1}h'\in H=(a^k)$，但 $0<i-j\leqslant k-1$，此与 $k=\min\{d\,\big|\,a^d\in H,d>0\}$(见第七章，二，3 的证明)矛盾. 所以 $Ha^i\cap Ha^j=\varnothing$. 因此，$Ha^0,Ha,Ha^2,\cdots,Ha^{k-1}$是 G 的一个分类，它们就是 G 的子群 H 的全部不同的右陪集，于是$[G:H]$有限且$[G:H]=k$.

证二　1)　还可如下证明唯一性.

已知$(a^s)<G$，$|(a^s)|=|a^s|=m$，$n=ms$.

若$(a^t)<G$，$|(a^t)|=|a^t|=m$，下面证明$(a^t)=(a^s)$. 因$a^{tm}=(a^t)^m=e$，又$|a|=n$，故$n\mid tm$，即$ms\mid tm$. 因$m\neq 0$，故$s\mid t$，于是$\exists q\in\mathbb{Z}$，使得$t=sq$. 因此$a^t=(a^s)^q\in(a^s)$，即$(a^t)\subset(a^s)$. 又$|(a^t)|=|(a^s)|=m$，所以$(a^t)=(a^s)$.

2）见证一.

注 利用该命题，容易求出n阶循环群的全部子群. 见如下例子.

例1 设$G=(a)$是6阶循环群. 6的正因子有且只有：1,2,3,6. 因此G的全部子群是4个循环群：H_1,H_2,H_3,H_4，它们的阶分别是1,2,3,6. $H_1=(e)=\{e\}$. 因G的2阶元只有a^3，故$H_2=(a^3)=\{e,a^3\}$. 因G的3阶元只有a^2,a^4，故$H_3=(a^2)=(a^4)=\{e,a^2,a^4\}$. 而$G$的6阶元有$a$与$a^5$，于是$H_4=(a)=(a^5)=G$.

例2 设$U_8=\left\{\varepsilon_k \middle| \varepsilon_k=\cos\frac{2k\pi}{8}+i\sin\frac{2k\pi}{8}.\ k=0,1,2,\cdots,7\right\}$是8次单位根乘群. 则$U_8=(\varepsilon_1)$是8阶循环群. 因8的正因子共有4个：1,2,4,8，故U_8恰有4个循环子群：$H_1=(\varepsilon_1^0)=\{1\}$，$H_2=(\varepsilon_1^4)=\{\varepsilon_1^0,\varepsilon_1^4\}$，$H_3=(\varepsilon_1^2)=\{\varepsilon_1^0,\varepsilon_1^2,\varepsilon_1^4,\varepsilon_1^6\}$，$H_4=(\varepsilon_1)=U_8$.

例3 设$G=(a)$是15阶循环群. 因15的正因子共有4个：1,3,5,15，故G有且只有4个循环子群：$H_1=(e)=\{e\}$，$H_2=(a^5)=\{e,a^5,a^{10}\}$，$H_3=(a^3)=\{e,a^3,a^6,a^9,a^{12}\}$，$H_4=(a)=G$.

例4 设$G=(a)$是100阶循环群. 因100的正因子共有9个：1,2,4,5,10,20,25,50,100，故G的全部子群是9个循环群：$H_1=(a^0)=\{e\}$，$H_2=(a^{50})$，$H_3=(a^{25})$，$H_4=(a^{20})$，$H_5=(a^{10})$，$H_6=(a^5)$，$H_7=(a^4)$，$H_8=(a^2)$，$H_9=(a)=G$，它们的阶分别是1,2,4,5,10,20,25,50,100.

3. 设群$G\neq\{e\}$，证明：

G除单位元群$\{e\}$和本身G外无其他子群$\Leftrightarrow G$是素数阶循环群.

证 （$\Leftarrow$） 由Lagrange定理得知.

（$\Rightarrow$） 因$G\neq\{e\}$，故$\exists x\in G$，而$x\neq e$，有$(x)<G$. 因$(x)\neq\{e\}$，故由已知，$(x)=G$，从而G是循环群. 下面证明$|x|=$素数. 事实上，假设不然，若$|x|=\infty$，则G有子群(x^2). 而$(x)^2\neq\{e\}$，又$(x^2)\neq(x)=G$，此与已知矛盾，于是$|x|$有限. 又$|x|\neq 1$，从而$|x|=$合数，于是$\exists$正整数l，且$l\neq 1$，$l\neq|x|$，使得$l\,\big|\,|x|$，$1<l<|x|$，从而G有子群(x^l). 但$|(x^l)|=|x^l|=\frac{|x|}{l}$既不等于1又不等于$|x|$，又产生了矛盾. 所以$|x|=$素数. 因此$G=(x)$是素数阶循环群.

注 第七章，二，6："素数阶群G是循环群"是该命题的一个特殊情况. 因素数的因子只有1与本身，故G只有$\{e\}$与本身是它的子群，从而由该命题的必要性知，G为循环群.

4. 设$H<G$，$K<G$且$|H|=m$，$|K|=n$，$(m,n)=1$，证明：$H\cap K=\{e\}$.

证一 $H\cap K<H$且$H\cap K<K$. 设$|H\cap K|=d$，则由Lagrange定理，$d\mid m$且$d\mid n$，从而$d\mid(m,n)=1$，于是$d=1$. 所以$H\cap K=\{e\}$.

证二 $\forall x\in H\cap K$，有$x\in H$且$x\in K$. 因此$|x|\,\big|\,m$且$|x|\,\big|\,n$，从而$|x|\,\big|\,(m,n)=1$. 于是$|x|=1$，所以$x=e$，即$H\cap K=\{e\}$.

证三 $\forall x\in H\cap K$，有$x\in H$且$x\in K$. 因此$x^m=e$且$x^n=e$（见第七章，三，1,7)).

因$(m,n)=1$，故$\exists s,t\in\mathbb{Z}$，使得$ms+nt=1$. 从而$x=x^{ms+nt}=(x^m)^s(x^n)^t=e^se^t=e$. 所

以 $H \cap K=\{e\}$.

注　该命题的逆命题不成立. 即:设 $H<G, K<G$ 且 $H \cap K=\{e\}$,未必$(|H|,|K|)=1$.

例　$G=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$,$H=\{(1),(1\ 2)(3\ 4)\}<G, K=\{(1),(1\ 3)(2\ 4)\}<G$ 且 $H \cap K=\{(1)\}$. 但$(|H|,|K|)=(2,2)\neq 1$.

5. 设 G 是有限群,且 $K<G, H<G, K \subset H$,证明:$[G:K]=[G:H][H:K]$.

证一　由 Lagrange 定理,有$|G|=|H|[G:H]$且$|G|=|K|[G:K]$. 因 $K<H$,故有 $|H|=|K|[H:K]$. 又$|K|\neq 0$,从而

$$[G:K]=\frac{|G|}{|K|}=\frac{|H|[G:H]}{|K|}=[G:H][H:K].$$

证二　设$[G:H]=s,[H:K]=t$,且 G 关于 H 的 s 个不同的右陪集为 $Ha_1, Ha_2, \cdots, Ha_s (a_1=e)$, H 关于 K 的 t 个不同的右陪集为 $Kb_1, Kb_2, \cdots, Kb_t (b_1=e)$. 即

$$G=Ha_1 \cup Ha_2 \cup \cdots \cup Ha_s,$$
$$H=Kb_1 \cup Kb_2 \cup \cdots \cup Kb_t.$$

我们只需证明 $Kb_ja_i(i=1,2,\cdots,s;j=1,2,\cdots,t)$是 G 关于 K 的所有不同的右陪集.

$\forall g \in G, g \in$某 Ha_i,从而 $g=ha_i, h \in H$. 而对于 h,又有 $h \in$某 kb_j,从而 $h=kb_j, k \in K$,所以 $g=kb_ja_i \in Kb_ja_i$,于是

$$\begin{aligned} G=&Kb_1a_1 \cup Kb_1a_2 \cup \cdots \cup Kb_1a_s \cup \\ &Kb_2a_1 \cup Kb_2a_2 \cup \cdots \cup Kb_2a_s \cup \\ &\cdots\cdots \\ &Kb_ta_1 \cup Kb_ta_2 \cup \cdots \cup Kb_ta_s \end{aligned}$$

下面再证明:当 $i \neq p$ 或 $j \neq q$ 时,有 $Kb_ja_i \cap Kb_qa_p=\varnothing$. 若 $i\neq p$,因 $Kb_j \subset H$,故 $Kb_ja_i \subset Ha_i$. 因 $Kb_q \subset H$,故 $Kb_qa_p \subset Ha_p$. 而 $Ha_i \cap Ha_p=\varnothing$,从而 $Kb_ja_i \cap Kb_qa_p=\varnothing$. 若 $i=p$,则 $j \neq q$. 如果$\exists x \in G$,而 $x \in Kb_ja_i \cap Kb_qa_p$,那么 $x \in Kb_ja_i$ 且 $x \in Kb_qa_p$. 于是 $x=kb_ja_i$ 且 $x=k'b_qa_p, k, k' \in K$, 从而 $xa_i=kb_j \in Kb_j$ 且 $xa_p=k'b_q \in kb_q$. 因此 $xa_i \in Kb_j \cap Kb_q$,这与 $Kb_j \cap Kb_q=\varnothing$矛盾. 所以 $Kb_ja_i \cap Kb_qa_p=\varnothing$.

综上所述,G 关于 K 的所有不同的右陪集. Kb_ja_i 恰为 st 个,所以$[G:K]=[G:H][H:K]$.

注　还可如下证明:当 $i\neq p$ 或 $j \neq q$ 时,$Kb_ja_i \cap Kb_qa_p=\varnothing$. 换句话说,只需证:如果 $Kb_ja_i=Kb_qa_p$,那么 $i=p$ 且 $j=q$. 事实上,若 $Kb_ja_i=Kb_qa_p$,则 $b_ja_i \in Kb_qa_p$,即 $b_ja_i=kb_qa_p, k \in K$. 又 $b_j, b_q, k \in H$,从而 $Ha_i=Hb_ja_i=Hkb_qa_p=Ha_p$,于是 $i=p$. 由 $b_ja_i=kb_qa_p$ 知 $b_j=kb_q$,因此 $Kb_j=Kkb_q=Kb_q$,于是 $j=q$.

四、思考问题

1. 试证明:

1)　2 次单位根乘群 $U_2=\{1,-1\}$是 4 次单位根乘群 $U_4=\{1,\mathrm{i},-\mathrm{i},-1\}$的子群. U_4 是 8 次单位根乘群 $U_8=\left\{1,\frac{1+\mathrm{i}}{\sqrt{2}},\mathrm{i},\frac{-1+\mathrm{i}}{\sqrt{2}},-\mathrm{i},\frac{-1-\mathrm{i}}{\sqrt{2}},-\mathrm{i},\frac{1-\mathrm{i}}{\sqrt{2}}\right\}$的子群.

2)　正有理数集 $\mathbb{Q}^+$ 是正实数乘群 $\mathbb{R}^+$ 的子群.

3)　$H=\left\{x \mid x=2^n, n \in \mathbb{Z}\right\}$是非零有理数乘群 $\mathbb{Q}^*$ 的一个子群.

4) $H=\left\{r+\mathrm{i}s \,\middle|\, r,s \text{ 是偶数}\right\}$是加法群$G=\left\{a+\mathrm{i}b \,\middle|\, a,b\in\mathbb{Z}\right\}$的一个子群.

5) $H=\left\{p^m q^n \,\middle|\, m,n\in\mathbb{Z}\right\}$($p,q$是两个不同的素数)是非零有理数乘群的一个子群.

6) $H=\left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \,\middle|\, a,b\in \text{数域 } Y, ab\neq 0\right\}$是乘法群$G=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \,\middle|\, \begin{pmatrix} a & b \\ c & c \end{pmatrix} \text{是 } Y \text{ 上 2 阶可逆方阵}\right\}$的一个子群.

7) 设$\mathbb{R}$是所有实数作成的集,则$H=\left\{\mathbb{R}\text{ 的变换 } \tau_{1b} \,\middle|\, \tau_{1b}: x\to x+b, b\in\mathbb{Q}\right\}$是对于变换乘法作成的群$G=\left\{\mathbb{R}\text{ 的变换 } \tau_{ab} \,\middle|\, \tau_{ab}: x\to ax+b, a,b\in\mathbb{Q}, a\neq 0\right\}$的一个子群.

8) 设G是交换群,n是固定正整数,则$H=\left\{h \,\middle|\, h\in G, h \text{ 使方程 } x^n=h \text{ 在 } G \text{ 中有解}\right\}$是$G$的一个子群.

9) 设G是交换群,则$H=\left\{x\in G \,\middle|\, x \text{ 的阶} \leqslant 2\right\}$是$G$的一个子群.

10) 取定$a\in$群G,则$H=\left\{a^n \,\middle|\, n\in\mathbb{Z}\right\}$是$G$的一个子群.

11) 设G是交换群,m是固定整数,则$G^{(m)}=\left\{x^m \,\middle|\, x\in G\right\}$是$G$的一个子群. $G_{(m)}=\left\{x\in G \,\middle|\, x^m=e\right\}$也是$G$的一个子群.

2. 设G是n阶循环群,$n=st$,H是G的t阶子群,证明:

1) H是G的元的s次幂的集合,即$H=\left\{x^s \,\middle|\, x\in G\right\}$.

2) H是G中阶为t的因子的元的集合,即$H=\left\{h\in G \,\middle|\, h^t=e\right\}$.

3. 试求出:

1) 由元$[25]$($\in\mathbb{Z}_{30}$)生成的循环子群.

2) 由集$S=\{2,3\}$($\subset$整数加群$\mathbb{Z}$)生成的子群.

3) 由集$S=\left\{p\in\mathbb{Q}^+ \,\middle|\, p \text{ 是素数}\right\}$($\subset$正有理数乘法群$\mathbb{Q}^+$)生成的子群.

4) 由集$S=\left\{1,\frac{1}{2},\frac{1}{3},\frac{1}{4},\cdots\right\}$($\subset$实数加法群$\mathbb{R}$)生成的子群.

5) 由集$S=\left\{a=\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, b=\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right\}$($\subset$完全线性群$GL_2(\mathbb{R})=\{A\in M_2(\mathbb{R}) \mid |A|\neq 0\}$)生成的子群.

6) 由集$S=\left\{A\in GL_n(\mathbb{R}) \,\middle|\, A \text{ 是初等矩阵}\right\}$($\subset$完全线性群$GL_n(\mathbb{R})$)生成的子群.

7) 由集$S=H\cup K$($\subset$加法群$M_n(\mathbb{R})$),其中$H=\left\{A\in M_n(\mathbb{R}) \,\middle|\, A'=A\right\}$,$K=\left\{B\in M_n(\mathbb{R}) \,\middle|\, B'=-B\right\}$生成的子群.

4. 设$a,b\in$群G,且$|a|=2$,$|b|=3$,$ab=ba$. 证明:由集$S=\{a,b\}$生成的子群$H=(S)$是循环群,并确定H的阶.

5. 设$H=\left\{a+b\sqrt{5} \,\middle|\, a,b\in\mathbb{Q}\right\}$对于数的加法作成一个群. $G=\left\{(a,b) \,\middle|\, a,b\in\mathbb{R}\right\}$对于

$$(a_1,b_1)=(a_2,b_2)\Leftrightarrow a_1=a_2 \text{ 且 } b_1=b_2,$$
$$(a_1,b_1)\oplus(a_2,b_2)=(a_1+a_2,b_1+b_2)$$

作成一个群. 试求 G 的一个子群 H',使 $H \cong H'$.

6. 对于命题:"设 $H<G$,则 G 的单位元 e 是 H 的单位元",下面的两种证法是否正确?

证法一　$\forall a \in H$,因 $H \subset G$,故 $a \in G$. 又因 e 是 G 的单位元,故 $ea=a$,从而 e 是 H 的单位元.

证法二　$\forall a \in H$,因 $H \subset G$,故 $a \in G$. 因 e 是 G 的单位元,故 $ea=a$,设 e'是 H 的单位元,则 $\forall a \in H$,有 $e'a=a$. 今有 $ea=a$,且 $e'a=a$,从而由 G 的单位元唯一知 $e=e'$. 所以 e 是 H 的单位元.

7. 设 G 是有限群,$H<G$,$a \in G$. 证明:存在最小正整数 m,使 $a^m \in H$ 且 m 是$|a|=n$ 的因数.

8. 证明:无限群 G 有无限个子群.

9. 证明:阶为合数的有限群 G 必有一个真子群.

10. 设 $H=(a^s)$,$K=(a^t)$是循环群 $G=(a)$的两个子群 . 证明:$H \cap K=(a^d)$,其中 d 是 s,t 的最小公倍数$[s,t]$.

11. 证明:任意一个群 G 都不能是它的两个真子群的并集.

12. 设有限集 $S=\{a_1,a_2,\cdots,a_k\}$是群 G 的不空子集,且 $a_ia_j=a_ja_i$,$|a_i|$有限,$i,j=1,2,\cdots,k$. 证明:(S)是有限交换群.

13. 试求出下列群 G 的子群 H 的全部右陪集.

1)　G 是 6 次单位根乘群$\left\{\varepsilon_k \,\middle|\, \varepsilon_k=\cos\frac{2k\pi}{6}+i\sin\frac{2k\pi}{6},k=0,1,2,3,4,5\right\}$. $H=\{\varepsilon_0,\varepsilon_3\}$.

2)　G 是 12 阶循环群$\{a^0=e,a,a^2,\cdots,a^{11}\}$. $H=\{e,a^4,a^8\}$.

3)　G 是整数加群. $H=\{4k \mid k \in G\}$.

4)　G 是非零有理数集对于数的乘法作成的群. $H=\{1,-1\}$.

5)　G 是非零有理数集对于数的乘法作成的群. H 是正有理数集对于数的乘法作成的群.

14. 设 $H_1<G$,$H_2<G$,证明:

1)　$H_1 \cap H_2$ 的任意一个右(左)陪集是 H_1 的一个右(左)陪集与 H_2 的一个右(左)陪集的交.

2)　若 H_1 与 H_2 在 G 里有有限指数,则 $H_1 \cap H_2$ 在 G 里也有有限指数.

15. 设 G 是 6 阶群,证明:G 至少含有一个 3 阶子群.

16. 设 $a,b \in$群 G,$|a|=$素数 p,$a \overline{\in} (b)$. 证明:$(a) \cap (b)=\{e\}$.

17. 交换群 G 中若$[G:G_{(k)}]$为有限数,证明:$G^{(k)}$ 为有限群,且$|G^{(k)}|=[G:G_{(k)}]$,其中 $G_{(k)}=\{x \in G \mid x^k=e\}$,$G^{(k)}=\{x^k \mid x \in G\}$.

18. 我们有如下结论:设 H 是群 G 的有限子群,则 H 的任意两个右陪集所含元素的个数相等. 当 G 不是群时,该命题是否仍成立?

19. 设 G 是有限交换群,d 是满足条件:$\forall a \in G$,$a^d=e$ 的最小正整数,则称 d 为 G 的指数. 设有限交换群 G 有$|G|=n$,证明:

$$G \text{ 是循环群} \Leftrightarrow G \text{ 的指数 } d=n.$$

20. 设有限交换群 G 中元的最大阶为 m. 证明:G 中任一元的阶是 m 的因数.

21. 设 H,K,N 是有限群 G 的子群,且 $K<H$,证明:$[H:K] \geqslant [N \cap H:N \cap K]$.

22. 设 $H<G$,$K<G$,证明:$[G:K] \geqslant [H:H \cap K]$.

第八章　不变子群、商群、同态与不变子群

一、基本问题问答

1. 举例说明下面命题："设 $N\lhd G, a\in G, an\in aN=Na$，则 $an=na$"不成立.

答　例，$N=\{(1),(1\ 2\ 3),(1\ 3\ 2)\}\lhd S_3$，$(1\ 2)\in S_3$，$(1\ 2)(1\ 2\ 3)\in(1\ 2)N$，因 $(1\ 2)N=N(1\ 2)$，故 $(1\ 2)(1\ 2\ 3)\in N(1\ 2)$，但 $(1\ 2)(1\ 2\ 3)=(1\ 3)\neq(2\ 3)=(1\ 2\ 3)(1\ 2)$.

正确的说法是：$\exists(1\ 3\ 2)\in N$，使得 $(1\ 2)(1\ 2\ 3)=(1\ 3\ 2)(1\ 2)$. 问题关键在于 $aN=Na$ 是指两个集合 aN 与 Na 相等，并不要求 $\forall n\in N$，都有 $an=na$.

2. 商群 G/N 的单位元是什么？$xN(\in G/N)$ 的逆元是什么？

答　G/N 的单位元是 $eN=N$. xN 的逆元 $(xN)^{-1}=x^{-1}N$.

3. 选择正确答案.

1)　商群 G/G 是(　　).

①　G；　②　$\{G\}$；　③　$\left\{\{x\}\middle|x\in G\right\}$；　④　$x(x\in G)$；　⑤　$\{e\}$；　⑥　e.

2)　商群 $G/\{e\}$ 是(　　).

①　G；　②　$\{G\}$；　③　$\left\{\{x\}\middle|x\in G\right\}$；　④　$x(x\in G)$；　⑤　$\{e\}$；　⑥　e.

答　1)　选②. 因 $G/G=\left\{aG\middle|a\in G\right\}=\{G\}$.

2)　选③. 因 $G/\{e\}=\left\{x\{e\}\middle|x\in G\right\}=\left\{\{xe\}\middle|x\in G\right\}=\left\{\{x\}\middle|x\in G\right\}$.

4. $N=\{(1),(1\ 4)(2\ 3)\}\lhd B_4=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$，问 B_4/N 中有哪些元素？

答

$(1)N=N=\{(1),(1\ 4)(2\ 3)\}=(1\ 4)(2\ 3)N.$

$$\begin{aligned}(1\ 2)(3\ 4)N&=\{(1\ 2)(3\ 4)(1),(1\ 2)(3\ 4)(1\ 4)(2\ 3)\}\\&=\{(1\ 2)(3\ 4),(1\ 3)(2\ 4)\}=(1\ 3)(2\ 4)N.\end{aligned}$$

$B_4/N=\left\{aN\middle|a\in G\right\}=\{N,(1\ 2)(3\ 4)N\}.$

5. 1)　$(3)=\left\{3q\middle|q\in\mathbb{Z}\right\}\lhd\mathbb{Z}$，$\mathbb{Z}/(3)=\mathbb{Z}_3=\{0+N,1+N,2+N\}=\{[0],[1],[2]\}$.

$$\phi:\ a\to a+(3)=[a]$$

是 $\mathbb{Z}$ 到 $\mathbb{Z}/(3)$ 的一个同态满射(称为自然同态). 证明：ϕ 的核 $\ker\phi=(3)$.

2)　一般来说，$N\lhd G$，ϕ：$a\to aN$ 是 G 到 G/N 的自然同态，则 $\ker\phi=N$.

证　1)　$\mathbb{Z}/(3)$ 的单位元是 (3). $\forall a\in\ker\phi$，有 $\phi(a)=(3)$. 又 $\phi(a)=[a]$，于是 $[a]=(3)$，因此 $a\in(3)$，从而 $\ker\phi\subset(3)$；反之，$\forall 3q\in(3)$，有 $\phi(3q)=3q+(3)=(3)$，因此 $3q\in\ker\phi$，从而 $(3)\subset\ker\phi$. 所以 $\ker\phi=(3)$.

2） 可仿 1)来证明．还可如下证明：由已知$\phi: a \to aN$ 知

$$\ker \phi = \{x \in G \mid \phi(x) = N\} = \{x \in G \mid xN = N\}$$
$$= \{x \in G \mid x \in N\} = N.$$

注 ① 由 1)可知，不变子群(3)不是有限群，但(3)在 $\mathbb{Z}$ 里的指数$[\mathbb{Z}:(3)] = |\mathbb{Z}/(3)| = 3$ 是有限正整数.

② 设群 $G \overset{\psi}{\sim} G/N$. 若 ψ 不是自然同态，未必有 $\ker \psi = N$.

例 取 $G = \{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$是 Klein 四元群．$N = \{(1),(1\ 3)(2\ 4)\} \lhd G$，则 $G/N = \{N,(1\ 2)(3\ 4)N\}$，$\psi$：$(1) \to N$，$(1\ 2)(3\ 4) \to N$，$(1\ 3)(2\ 4) \to (1\ 2)(3\ 4)N$，$(1\ 4)(2\ 3) \to (1\ 2)(3\ 4)N$ 是 G 到 G/N 的同态满射，但 $\ker \psi = \{(1),(1\ 2)(3\ 4)\} \neq N$.

6. 设 $GL_n(\mathbb{R}) = \{X \mid X$ 是$\mathbb{R}$上 n 阶可逆方阵$\}$是 n 次完全线性群．$SL_n(\mathbb{R}) = \{X \in GL_n(\mathbb{R}) \mid |x| = 1\}$是 n 次特殊线性群．证明：

1） $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$.

2） 若$\mathbb{R}^*$是非零实数集对于普通乘法作成的群，则 $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^*$.

证 1） 因 n 阶单位矩阵$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \in SL_n(\mathbb{R})$，故 $SL_n(\mathbb{R}) \neq \varnothing$，显然 $SL(\mathbb{R}) \subset GL_n(\mathbb{R})$.

$\forall X, Y \in SL_n(\mathbb{R})$，$|XY| = |X||Y| = |X| = 1$，于是 $XY \in SL_n(\mathbb{R})$．$\forall X \in SL_n(\mathbb{R})$，$|X^{-1}| = |X|^{-1} = 1^{-1} = 1$，于是 $X^{-1} \in SL_n(\mathbb{R})$．所以 $SL_n(\mathbb{R}) < GL_n(\mathbb{R})$.

$\forall X \in GL_n(\mathbb{R})$，$N \in SL_n(\mathbb{R})$，$|XNX^{-1}| = |X||N||X^{-1}| = |X| \cdot 1 \cdot |X|^{-1} = 1$，于是 $XNX^{-1} \in SL_n(\mathbb{R})$．所以 $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$.

2） $\phi: X \to |X|$是 $GL_n(\mathbb{R})$到$\mathbb{R}^*$的一个同态满射，即 $GL_n(\mathbb{R}) \overset{\phi}{\sim} \mathbb{R}^*$．下面证明 $\ker \phi = SL_n(\mathbb{R})$．事实上，群$\mathbb{R}^*$的单位元是 1.

$$X \in \ker \phi \Leftrightarrow \phi(X) = 1 \xLeftrightarrow{\phi(X)=|X|} |X| = 1 \Leftrightarrow X \in SL_n(\mathbb{R}),$$

从而$\ker\phi = SL_n(\mathbb{R})$．由同态基本定理，$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \overset{\psi}{\cong} \mathbb{R}^*$．同构映射$\psi: XSL_n(\mathbb{R}) \to \overline{X} = \phi(X) = |X|$.

注 同态基本定理是群论中最重要的定理之一．许多涉及群的同态或同构问题都要用此定理来解决.

7. 1） 设 G 是一个群．取定 $x \in G$，$a \in G$，称 axa^{-1} 为 x 的共轭元.

2） 设 $H < G$，取定 $a \in G$，易证 $aHa^{-1} < G$. 称 aHa^{-1} 为 H 的共轭子群.

3） 取定 $a \in G$，易证

$$\phi_a: x \to axa^{-1}（x\text{ 的共轭元}）$$

是 G 的一个自同构，称ϕ_a 是 G 的一个内自同构.

记子群 H 在内自同构ϕ_a 下的象为$\phi_a(H) = \{aha^{-1} \mid h \in H\}$（$H$ 的共轭子群）.

证明：

① $H \lhd G \Leftrightarrow \forall a \in G, \phi_a(H)=H$.

② $|H|=|aHa^{-1}|, a \in G$.

证 ①

$$H \lhd G \Leftrightarrow \forall a \in G, aHa^{-1}=H^{①}$$

$$\xLeftrightarrow[aHa^{-1}=\phi_a(H)]{} \forall a \in G, \phi_a(H)=H.$$

② 显然$\phi: h \to aha^{-1}$是 H 与 aHa^{-1}间的一个一一映射,从而$|H|=|aHa^{-1}|$.

注 1) 结论①说明,在群 G 的所有内自同构下都不变的子群是不变子群．这就说明了不变子群的名称的含义．不变子群也称正规子群.

2) 设 $H<G$,则

$$H \lhd G \Leftrightarrow H \text{ 与它的所有共轭子群重合}$$
$$\Leftrightarrow H \text{ 的共轭子群只有一个,就是 } H \text{ 自己}.$$

因此不变子群也称自共轭子群.

3) 设 $H<G$,则

$$H \lhd G \Leftrightarrow H \text{ 由其中每个元的所有共轭元组成}$$
$$\Leftrightarrow H \text{ 包含其中每个元 } h \text{ 的所有共轭元 } aha^{-1}(\forall a \in G).$$

因此 G 的一个元的所有共轭元或都属于某一不变子群,或都不属于该不变子群.

二、典型问题分析

1. 假定群 G 的不变子群 N 的阶是 2. 证明:G 的中心包含 N.

证一 因$|N|=2$,故可设 $N=\{e,n\}$. 因 $N \lhd G$,故 $\forall a \in G, aN=Na$,即$\{ae,an\}=\{ea,na\}$,从而 $ae=a=ea, an=na$,于是 e,n 都 $\in G$ 的中心．所以 $N \subset G$ 的中心.

证二 设 $N=\{e,n\}$. 因 $N \lhd G$,故$\forall a \in G$,有 $ana^{-1} \in N$. 若 $ana^{-1}=e$,则 $an=a$. 由消去律,$n=e$,此为不可能,从而 $ana^{-1}=n$,于是 $an=na$,因此 $n \in G$ 的中心．又 $ae=ea, \forall a \in G$,可见 $e \in G$ 的中心．所以 $N \subset G$ 的中心.

注 条件“N 的阶是 2”不能去掉．即命题“设 $N \lhd G$,则 G 的中心 $Z \supset N$”不成立．例,$N=\{(1),(1\ 2\ 3),(1\ 3\ 2)\} \lhd S_3$,$S_3$ 的中心 $Z=\{(1)\}$,但 $Z \not\supset N$.

2. 证明:两个不变子群的交集还是不变子群.

证一 设 $N_1 \lhd G, N_2 \lhd G$,则由第七章、二,2,$N_1 \cap N_2 < G$. $\forall a \in G, n \in N_1 \cap N_2$,有 $n \in N_1$ 且 $n \in N_2$. 由 $N_1 \lhd G$ 且 $N_2 \lhd G$,$ana^{-1} \in N_1$ 且 $ana^{-1} \in N_2$,从而 $ana^{-1} \in N_1 \cap N_2$. 所以 $N_1 \cap N_2 \lhd G$.

证二 设 $N_i \lhd G, i=1,2$,则由第七章,二,2,$N_1 \cap N_2 < G$,且$\forall x \in G, N_i x = xN_i, i=1,2$. 再由第七章,四,14,1),$(N_1 \cap N_2)x = N_1 x \cap N_2 x = xN_1 \cap xN_2 = x(N_1 \cap N_2)$, $\forall x \in G$. 所以,$N_1 \cap N_2 \lhd G$.

注 1) 群 G 中任意多个(有限或无限)不变子群的交仍是 G 的不变子群.

2) 设 $H<G, N \lhd G$,则 $H \cap N \lhd H$. 事实上,$H \cap N < G$, $H \cap N \subset H$,且 $H<G$,从而

① 张禾瑞．近世代数基础．北京:高等教育出版社,1978. 72. 定理 1.

$H\cap N<H$. $\forall h\in H$, $\forall a\in H\cap N$，由 $h\in G$, $a\in N$, $N\lhd G$ 知，$hah^{-1}\in N$，由 $h\in H$, $a\in H$, $H<G$，知 $hah^{-1}\in H$. 于是 $hah^{-1}\in H\cap N$，所以 $H\cap N\lhd H$.

3) 命题："$H<G, N\lhd G\Rightarrow H\cap N\lhd G$"不对．例，$H=\{(1),(1\ 2)\}<S_3$, $S_3\lhd S_3$, $H\cap S_3=H$，但 H 不是 S_3 的不变子群.

4) 命题："$H<G, K<G$ 且 $H\cap K\lhd H\Rightarrow K\lhd G$"不对．例，$H=\{(1),(12)\}<S_3$, $K=\{(1),(13)\}<S_3$，且 $H\cap K=\{(1)\}\lhd H$. 但 K 不是 S_3 的不变子群.

5) 两个不变子群的并集未必是不变子群．例，见第七章，二，2，注 1).

3. 证明：指数是 2 的子群一定是不变子群.

证一　设 H 是群 G 的指数是 2 的子群，则 H 有且只有两个左陪集 eH, aH，两个右陪集 He, Ha，且 $eH\cup aH=G=He\cup Ha$, $eH\cap aH=\varnothing=He\cap Ha$，这里 $a\in G$ 而 $a\overline{\in}H$. 显然 $eH=He=H$，从而

$$aH=G-eH=G-He=Ha.$$

所以 $\forall x\in G$，都有 $xH=Hx$. 因此 $H\lhd G$.

证二　设 $H<G$, $[G:H]=2$，则 H 有且只有两个右陪集 He, Ha，两个左陪集 eH, aH，这里 $a\in G$ 而 $a\overline{\in}H$. 因 $He=eH$，故只需证 $Ha=aH$.

$\forall b\in Ha$，因 $He\cap Ha=\varnothing$，故 $b\overline{\in}He$，即 $b\overline{\in}eH$. 又 $eH\cup aH=G$，从而 $b\in aH$. 所以 $Ha\subset aH$. 类似可证 $aH\subset Ha$. 因此 $aH=Ha$. 于是 $H\lhd G$.

注　该命题的逆命题不成立．例，$N=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}\lhd S_4$，而 $[S_4:N]=\frac{24}{4}=6\neq 2$.

4. 假定 H 是 G 的子群，N 是 G 的不变子群．证明：HN 是 G 的子群.

证一　$HN\subset G$. 因 $e=ee\in HN$，故 $HN\neq\varnothing$.

1) $\forall h_1n_1, h_2n_2\in HN$, $(h_1n_1)(h_2n_2)=h_1(n_1h_2)n_2$. 因 $N\lhd G$，故 $n_1h_2\in Nh_2=h_2N$，从而 $\exists n_3\in N$，使得 $n_1h_2=h_2n_3$. 于是 $(h_1n_1)(h_2n_2)=(h_1h_2)(n_3n_2)\in HN$.

2) $\forall hn\in HN$. 因 $N\lhd G$，故 $(hn)^{-1}=n^{-1}h^{-1}\in Nh^{-1}=h^{-1}N$，从而 $\exists n_4\in N$，使得 $(hn)^{-1}=h^{-1}n_4\in HN$(或 $(hn)^{-1}=n^{-1}h^{-1}=h^{-1}(hn^{-1}h^{-1})\in HN$). 所以 $HN<G$.

证二　$\varnothing\neq HN\subset G$. $\forall h_1n_1, h_2n_2\in HN$, $(h_1n_1)(h_2n_2)^{-1}=h_1(n_1n_2^{-1}h_2^{-1})$. 因 $N\lhd G$，故 $n_1n_2^{-1}h_2^{-1}\in Nh_2^{-1}=h_2^{-1}N$，从而 $\exists n\in N$，使得 $n_1n_2^{-1}h_2^{-1}=h_2^{-1}n$. 于是 $(h_1n_1)\cdot(h_2n_2)^{-1}=h_1h_2^{-1}n\in HN$[或 $(h_1n_1)(h_2n_2)^{-1}=h_1n_1n_2^{-1}h_2^{-1}=h_1h_2^{-1}(h_2n_1h_2^{-1})(h_2n_2^{-1}\cdot h_2^{-1})\in HN$，这是因为 $N\lhd G$，所以 $h_2n_1h_2^{-1}, h_2n_2^{-1}h_2^{-1}\in N$]. 于是 $HN<G$.

注　1) 若 $H\lhd G$, $N<G$，则同理有 $HN<G$.

2) 命题："设 $H<G$, $K<G$，则 $HK<G$"不成立．例，$H=\{(1),(1\ 2)\}<S_3$, $K=\{(1),(1\ 3)\}<S_3$，但 $HK=\{(1),(1\ 2),(1\ 3),(1\ 2\ 3)\}$ 不是 S_3 的子群．因为 $(1\ 2\ 3)(1\ 2\ 3)=(1\ 3\ 2)\overline{\in}HK$. 又例，$H=\left\{\begin{pmatrix}1&0\\0&a\end{pmatrix}\middle| a\in\mathbf{R}, a\neq 0\right\}<GL_2(\mathbf{R})$，$K=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix}\right\}<GL_2(\mathbf{R})$，但 $HK=\left\{\begin{pmatrix}1&0\\0&a\end{pmatrix}\middle| a\in\mathbf{R}, a\neq 0\right\}\cup\left\{\begin{pmatrix}0&1\\b&0\end{pmatrix}\middle| b\in\mathbf{R}, b\neq 0\right\}$ 不是 $GL_2(\mathbf{R})$ 的子群．因为 $\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}1&0\\0&2\end{pmatrix}\in HK$，而 $\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&0\\0&2\end{pmatrix}=\begin{pmatrix}0&2\\1&0\end{pmatrix}\overline{\in}HK$，即 HK

对于矩阵乘法不封闭.

3) 该命题中条件“$N \lhd G$”是充分的,而不是必要的,即:设 $H<G,N<G$,且 $HN<G$,但 N 与 H 未必是 G 的不变子群. 例,$H=\{(1),(1\ 2)(3\ 4)\}<S_4$,$N=\{(1),(1\ 3)(2\ 4)\}<S_4$,且 $HN=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}<S_4$,但 N 不是 S_4 的不变子群. 因为 $(1\ 3\ 2\ 4)N=\{(1\ 3\ 2\ 4),(3\ 4)\}$,而 $N(1324)=\{(1\ 3\ 2\ 4),(1\ 2)\}$,所以 $(1\ 3\ 2\ 4)N\neq N(1\ 3\ 2\ 4)$. H 也不是 S_4 的不变子群. 因为 $(1\ 2\ 3\ 4)H=\{(1\ 2\ 3\ 4),(2\ 4)\}$,而 $H(1\ 2\ 3\ 4)=\{(1\ 2\ 3\ 4),(1\ 3)\}$,所以 $(1\ 2\ 3\ 4)H\neq H(1\ 2\ 3\ 4)$. 因此要保证 $HN<G$,条件 $N\lhd G$ 太强,可以削弱.

4) 分析该命题的证明,可见“对于 $h\in H,n\in N,\exists n'\in N$,使得 $nh=hn'$”这一事实在证明中起了决定性的作用. 实际上,我们只需利用“对于 $h\in H,n\in N,\exists h'\in H,n'\in N$,使得 $nh=h'n'$”就可证明 $HN<G$. 因此只要求 $HN=NH$. 从而有下面的命题:设 $H<G,K<G$,则

$$HK=KH\Leftrightarrow HK<G.$$

证一 ($\Rightarrow$) $HK\subset G$. 因 $e=ee\in HK$. 故 $HK\neq\varnothing$. $\forall h_1k_1,h_2k_2\in HK$,$h_1k_1h_2k_2=h_1(k_1h_2)k_2$. 因 $k_1h_2\in KH=HK$. 故 $\exists h_3\in H,k_3\in K$,使得 $k_1h_2=h_3k_3$. 于是 $h_1k_1h_2k_2=(h_1h_3)(k_3k_2)\in HK$. $\forall hk\in HK$,$(hk)^{-1}=k^{-1}h^{-1}\in KH=HK$. 所以 $HK<G$.

($\Leftarrow$) $\forall kh\in KH$,$kh=((kh)^{-1})^{-1}=(h^{-1}k^{-1})^{-1}$,其中 $h^{-1}k^{-1}\in HK$. 又 $HK<G$,从而 $kh=(h^{-1}k^{-1})^{-1}\in HK$. 于是 $KH\subset HK$. 反之,$\forall hk\in HK$. $hk=((hk)^{-1})^{-1}=(k^{-1}h^{-1})^{-1}$. 因 $k^{-1}h^{-1}\in KH$,又已证得 $KH\subset HK$,故 $k^{-1}h^{-1}\in HK$. 因此 $\exists h_1\in H,k_1\in K$,使得 $k^{-1}h^{-1}=h_1k_1$,从而 $hk=(k^{-1}h^{-1})^{-1}=(h_1k_1)^{-1}=k_1^{-1}h_1^{-1}\in KH$. 于是 $HK\subset KH$. 所以 $HK=KH$.

证二 ($\Rightarrow$) 由证一知 $\varnothing\neq HK\subset G$. $\forall h_1k_1,h_2k_2\in HK$,$(h_1k_1)(h_2k_2)^{-1}=h_1k_1k_2^{-1}h_2^{-1}$. 因 $k_1k_2^{-1}h_2^{-1}\in KH=HK$,故 $\exists h'\in H,k'\in K$,使得 $k_1k_2^{-1}h_2^{-1}=h'k'$. 于是 $(h_1k_1)(h_2k_2)^{-1}=h_1h'k'\in HK$. 所以 $HK<G$.

($\Leftarrow$) $\forall kh\in KH$,$kh=(ek)(he)$. 因 $ek,he\in HK$,又 $HK<G$,故 $kh=(ek)(he)\in HK$. 于是 $KH\subset HK$. 反之,$\forall hk\in HK$,因 $HK<G$,故 $(hk)^{-1}\in HK$. 因此 $\exists h_1\in H,k_1\in K$,使得 $(hk)^{-1}=h_1k_1$,从而 $hk=((hk)^{-1})^{-1}=(h_1k_1)^{-1}=k_1{}^{-1}h_1{}^{-1}\in KH$. 于是 $HK\subset KH$. 所以 $HK=KH$.

证三 ① 设 $\varnothing\neq X\subset$ 群 G,规定 $X^{-1}=\{x^{-1}\mid x\in X\}$. 则有 $(AB)^{-1}=B^{-1}A^{-1}$,这里 $A\subset G,B\subset G$. 事实上,$(AB)^{-1}=\{(ab)^{-1}\mid a\in A,b\in B\}=\{b^{-1}a^{-1}\mid a\in A,b\in B\}=B^{-1}A^{-1}$.

② 易知:设 $\varnothing\neq H\subset$ 群 G,则 $H<G\Leftrightarrow HH=H$,且 $H^{-1}=H$①.

③ 下面证明:设 $H<G,K<G$,则

$$HK=KH\Leftrightarrow HK<G.$$

($\Rightarrow$) 显然 $\varnothing\neq HK\subset G$. 由已知 $HK=KH$,有 $(HK)(HK)=H(KH)K=H(HK)K=(HH)(KK)=HK$. 同时 $(HK)^{-1}=K^{-1}H^{-1}=KH=HK$. 所以由②知 $HK<G$.

($\Leftarrow$) 由 $HK<G$,有 $HK=(HK)^{-1}=K^{-1}H^{-1}=KH$.

由此注 4)知,交换群的任意两个子群的乘积还是子群.

---

① 张禾瑞. 近世代数基础. 北京:高等教育出版社. 1978. 62. 定理 1.

5）　注 4)可推广为：设 $H_1,H_2,\cdots,H_n$ 都是群 G 的子群，且 $H_1,H_2,\cdots,H_n$ 两两可换，则 $H_1H_2\cdots H_n<G$.

证　对 n 作数学归纳法.

①　$n=2$ 时，由注 4)，$H_1H_2<G$.

②　假定 $n-1$ 时命题成立．今看 n 时．设 $H_1,H_2,\cdots,H_n$ 是 G 的子群，且 $H_1,H_2,\cdots,H_n$ 两两可换，由归纳假定，$H_1H_2\cdots H_{n-1}<G$. 又 $H_n<G$，且 $(H_1H_2\cdots H_{n-1})H_n=H_n(H_1H_2\cdots H_{n-1})$. 所以由注 4)$H_1H_2\cdots H_{n-1}H_n<G$.

6）　利用注 4)，容易证明：设 $H<G,N\lhd G$，则 $HN<G$. 事实上，因 $N\lhd G$，故 $\forall h\in H\subset G$，都有 $hN=Nh$. 而 HN 是所有集合 $hN(\forall h\in H)$ 的并集，NH 是所有集合 $Nh(\forall h\in H)$ 的并集，因此 $HN=NH$. 由注 4)，$HN<G$.

由该证明知，设 $H<G$. 若 $N\lhd G$，则必可推出 $HN=NH$. 但其逆命题不成立(见注 3)).

7）　设 $H<G,K<G$，则 $HK=KH\Leftrightarrow (H\cup K)=HK$.

证一　($\Rightarrow$)　因 $HK=KH$，故由注 4)知，$HK<G$. HK 含 H 也含 K，因此 HK 是含 $H\cup K$ 的子群．而$(H\cup K)$是含 $H\cup K$ 的最小子群，于是$(H\cup K)\subset HK$. 另一方面，$\forall hk\in HK$，都有 $hk\in(H\cup K)$. 于是 $HK\subset(H\cup K)$. 所以$(H\cup K)=HK$.

($\Leftarrow$)　因 $HK=(H\cup K)$，故 $HK<G$，由注 4)，$HK=KH$.

证二　($\Rightarrow$)　$\forall g_1g_2\cdots g_n\in(H\cup K)$，$g_i\in H\cup K$ 即 $g_i\in H$ 或 $g_i\in K$. 因 $HK=KH$，故 $g_1g_2\cdots g_n$ 总可写成 $hk(h\in H,k\in K)$ 形，从而 $g_1g_2\cdots g_n\in HK$，于是$(H\cup K)\subset HK$. 显然有 $HK\subset(H\cup K)$. 所以$(H\cup K)=HK$.

($\Leftarrow$)　见证一.

8）　设 $H<G,K<G,K\lhd(H\cup K)$，则 ①　$(H\cup K)=HK$. ②　$H\cap K\lhd H$.

证一　①　因 $H<G,H\subset(H\cup K)$，故 $H<(H\cup K)$. 又 $K\lhd(H\cup K)$，从而 $HK<(H\cup K)$. 因$(H\cup K)<G$，故 $HK<G$. 由注 4)，$HK=KH$，再由注 7)，$(H\cup K)=HK$.

②　显然 $H\cap K<H$. $\forall x\in H\cap K,h\in H$，有 $x\in H$，此时 $hxh^{-1}\in H$. 又 $x\in K,h\in(H\cup K)$且 $K\lhd(H\cup K)$，从而 $hxh^{-1}\in K$. 于是 $hxh^{-1}\in H\cap K$. 所以 $H\cap K\lhd H$.

证二　①　显然 $HK\subset(H\cup K)$. 另一方面，$\forall x_1x_2\cdots x_n\in(H\cup K)$，$x_i\in H\cup K$，即 $x_i\in H$或 $x_i\in K$. 因 $K\lhd(H\cup K)$，$H\subset(H\cup K)$，故 $x_1x_2\cdots x_n$ 总可表为 $hk(h\in H,k\in K)$ 形，从而$x_1x_2\cdots x_n\in HK$. 于是$(H\cup K)\subset HK$. 所以$(H\cup K)=HK$.

②　见证一.

9）　设 $H<G,K<G,HK=KH$，则 $K<HK$.

证　由 $HK=KH$ 及注 4)，$HK<G$. 又 $K=Ke\subset KH$ 且 $K<G$，从而 $K<HK$.

10）　设 $N_1\lhd G,N_2\lhd G$，则 $N_1N_2\lhd G$.

证一　显然 $N_1N_2<G$. $\forall x\in G$，因 $N_1\lhd G,N_2\lhd G$，故 $x(N_1N_2)x^{-1}=(xN_1x^{-1})\cdot(xN_2x^{-1})=N_1N_2$. 所以 $N_1N_2\lhd G$.

证二　显然 $N_1N_2<G$. $\forall x\in G,n_1n_2\in N_1N_2$，因 $N_1\lhd G,N_2\lhd G$，故 $xn_1n_2x^{-1}=(xn_1x^{-1})\cdot(xn_2x^{-1})\in N_1N_2$. 所以 $N_1N_2\lhd G$.

证三　显然 $N_1N_2<G$. $\forall x\in G,n_1n_2\in N_1N_2$. 因 $N_1\lhd G$，故 $xn_1\in xN_1=N_1x$，从而 $\exists n_1'\in N_1$，使得 $xn_1=n_1'x$. 又因 $N_2\lhd G$，故 $xn_2\in xN_2=N_2x$，从而 $\exists n_2'\in N_2$，使得 $xn_2=n_2'x$. 于是 $xn_1n_2x^{-1}=n_1'xn_2x^{-1}=n_1'n_2'xx^{-1}=n_1'n_2'\in N_1N_2$. 所以 $N_1N_2\lhd G$.

可推广为：群 G 的任意多个不变子群的乘积仍是 G 的不变子群.

11） 命题"$N_1 \lhd G, N_2 < G \Rightarrow N_1N_2 \lhd G$"不成立．例，$\{(1)\} \lhd S_3$，$\{(1),(1\ 2)\} < S_3$，但 $\{(1)\}\{(1),(1\ 2)\} = \{(1),(1\ 2)\}$ 不是 S_3 的不变子群.

12） 设 $N \lhd G, H < G$，则 $N \lhd HN$.

证 显然 $HN < G$，又 $N = eN \subset HN$，$N < G$，从而 $N < HN$. $\forall x \in HN \subset G$，因 $N \lhd G$，故 $xN = Nx$. 所以 $N \lhd HN$.

13） 设 $N_i \lhd G(i=1,2,\cdots,s)$，则 $N_1N_2\cdots N_s = (N_1 \cup N_2 \cup \cdots \cup N_s)$.

证一 显然 $N_1N_2\cdots N_s \subset (N_1 \cup N_2 \cup \cdots \cup N_s)$. 反之，$\forall n_{i_1}n_{i_2}\cdots n_{i_t} \in (N_1 \cup N_2 \cup \cdots \cup N_s)$.

① 若 $i_1 \leqslant i_2 \leqslant \cdots \leqslant i_t$，则显然 $n_{i_1}n_{i_2}\cdots n_{i_t} \in N_1N_2\cdots N_s$.

② 若有某 $i_l > i_{l+1}$. 因 $N_{i_l} \lhd G$，故 $n_{i_l}n_{i_{l+1}} \in N_{i_l}n_{i_{l+1}} = n_{i_{l+1}}N_{i_l}$，从而 $\exists n'_{i_l} \in N_{i_l}$，使得 $n_{i_l}n_{i_{l+1}} = n_{i_{l+1}}n'_{i_l}$. 因此总可使下标 i_j 按从小到大的次序排好，从而也有 $n_{i_1}n_{i_2}\cdots n_{i_t} \in N_1N_2\cdots N_s$.

于是 $(N_1 \cup N_2 \cup \cdots \cup N_s) \subset N_1N_2\cdots N_s$. 所以 $N_1N_2\cdots N_s = (N_1 \cup N_2 \cup \cdots \cup N_s)$.

证二 $(N_1 \cup N_2 \cup \cdots \cup N_s)$ 是含 $N_1 \cup N_2 \cup \cdots \cup N_s$ 的 G 的最小子群．$N_1N_2\cdots N_s$ 是含 $N_1 \cup N_2 \cup \cdots \cup N_s$ 的 G 的子集．下面证明 $N_1N_2\cdots N_s < G$. 事实上，$\forall n_1n_2\cdots n_s, n_1'n_2'\cdots n_s' \in N_1N_2\cdots N_s$. 因 $N_i \lhd G$，故 $n_in_j' \in N_in_j' = n_j'N_i$，从而 $\exists n_i^{(0)} \in N_i$，使得 $n_in_j' = n_j'n_i^{(0)}$，因此 $(n_1n_2\cdots n_s)(n_1'n_2'\cdots n_s')$ 总可写成 $n_1''n_2''\cdots n_s''$ ($n_i'' \in N_i, i=1,2,\cdots,s$) 形．于是有 $(n_1n_2\cdots n_s) \cdot (n_1'n_2' \cdot \cdots n_s') = n_1''n_2''\cdots n_s'' \in N_1N_2\cdots N_s$. $\forall n_1n_2\cdots n_s \in N_1N_2\cdots N_s$，同理，有 $(n_1n_2\cdots n_s)^{-1} = n_s^{-1}n_{s-1}^{-1}\cdots n_1^{-1} = n_1'''n_2'''\cdots n_s''' \in N_1N_2\cdots N_s$. 所以 $N_1N_2\cdots N_s < G$. 于是 $(N_1 \cup N_2 \cup \cdots \cup N_s) \subset N_1N_2\cdots N_s$. 显然有 $N_1N_2\cdots N_s \subset (N_1 \cup N_2 \cup \cdots \cup N_S)$. 因此 $N_1N_2\cdots N_s = (N_1 \cup N_2 \cup \cdots \cup N_s)$.

证三 对 s 作数学归纳法.

① $s=2$ 时，因 $N_1 \lhd G, N_2 \lhd G$，由注 10)，$N_1N_2 < G$，由注 4)，$N_1N_2 = N_2N_1$，由注 7)，$N_1N_2 = (N_1 \cup N_2)$.

② 假定 $s-1$ 时命题成立．今证 s 时命题也成立．设 $N_i \lhd G(i=1,2,\cdots,s)$，由归纳假定，$N_1N_2\cdots N_{s-1} = (N_1 \cup N_2 \cup \cdots \cup N_{s-1})$，从而 $N_1N_2\cdots N_{s-1} < G$，因此 $(N_1N_2\cdots N_{s-1})N_s < G$. 由注 4)，$(N_1N_2\cdots N_{s-1})N_s = N_s(N_1N_2\cdots N_{s-1})$，由注 7)，$N_1N_2\cdots N_s = (N_1N_2\cdots N_{s-1})N_s = (N_1N_2\cdots N_{s-1} \cup N_s) = ((N_1 \cup N_2 \cup \cdots \cup N_{s-1}) \cup N_s) = (N_1 \cup N_2 \cup \cdots \cup N_{s-1} \cup N_s)$.

14） 命题"设 $H < G$，$K < G$ 且 $ab \in HK$，则 $a \in H$，$b \in K$"不对．例，$H = \left\{\begin{pmatrix} a & b \\ o & a \end{pmatrix} \middle| a, b \in \mathbf{R}, a \neq 0\right\} < GL_2(\mathbf{R})$，$K = \left\{\begin{pmatrix} a & o \\ b & a \end{pmatrix} \middle| a, b \in \mathbf{R}, a \neq 0\right\} < GL_2(\mathbf{R})$. $\begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}\begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in HK$，但 $\begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} \overline{\in} H$，$\begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix} \overline{\in} K$，而是 $\exists \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$，$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in K$，使得 $\begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}\begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

5. 举例证明：G 的不变子群 N 的不变子群 N_1 未必是 G 的不变子群.

证 例，取 $G = S_4$，$N = \{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$ 是 Klein 四元群，又 $N \subset S_4$，从而 $N < S_4$，下面证明 $N \lhd S_4$. 我们注意到 N 中除 (1) 以外，其余 3 个元都具有形式 $(ij)(kl)$，这里 i,j,k,l 两两不等．又 $\forall \pi = \begin{pmatrix} i_1 & i_2 & i_3 & i_4 \\ i_1' & i_2' & i_3' & i_4' \end{pmatrix} \in G$，经验证，有

$$\pi(i_1'i_2')(i_3'i_4')\pi^{-1} = (i_1i_2)(i_3i_4) \in N,$$

$$\pi(i_1'i_3')(i_2'i_4')\pi^{-1}=(i_1i_3)(i_2i_4)\in N,$$
$$\pi(i_1'i_4')(i_2'i_3')\pi^{-1}=(i_1i_4)(i_2i_3)\in N,$$
$$\pi(1)\pi^{-1}=(1)\in N.$$

因此，$\forall\pi\in G$，$\forall n\in N$，都有 $\pi n\pi^{-1}\in N$. 所以，$N\lhd G$. 取 $N_1=\{(1),(1\ 4)(2\ 3)\}$. 因 $\forall n\in N_1$，有$(1)n=n(1)=n\in N_1$，$[(1\ 4)(2\ 3)]^2=(1)\in N_1$，故 N_1 对于 N 的乘法封闭．又 N_1 是 N 的有限不空子集，从而 $N_1<N$. 因 N 是交换群，故 $N_1\lhd N$. 但 N_1 不是 G 的不变子群．因取$(3\ 4)\in G$，$(1\ 4)(2\ 3)\in N_1$，有$(3\ 4)[(1\ 4)(2\ 3)](3\ 4)^{-1}=(1\ 3)(2\ 4)\overline{\in} N_1$.

又例，$G=\left\{\begin{pmatrix}a&b\\0&1\end{pmatrix}\middle|\,a,b\in\mathbb{Q},a\neq0\right\}$对于矩阵乘法作成一个群．$N=\left\{\begin{pmatrix}1&c\\0&1\end{pmatrix}\middle|\,c\in\mathbb{Q}\right\}$，$N_1=\left\{\begin{pmatrix}1&n\\0&1\end{pmatrix}\middle|\,n\in\mathbb{Z}\right\}$. 则 1)　$N\lhd G$. 2)　$N_1\lhd N$. 3)　N_1 不是 G 的不变子群．事实上，

1)　因$\begin{pmatrix}1&0\\0&1\end{pmatrix}\in N$，故 $N\neq\varnothing$ 且 $N\subset G$. $\forall\begin{pmatrix}1&c\\0&1\end{pmatrix},\begin{pmatrix}1&c'\\0&1\end{pmatrix}\in N$，$\begin{pmatrix}1&c\\0&1\end{pmatrix}\begin{pmatrix}1&c'\\0&1\end{pmatrix}^{-1}=$ $\begin{pmatrix}1&c\\0&1\end{pmatrix}\begin{pmatrix}1&-c'\\0&1\end{pmatrix}=\begin{pmatrix}1&-c'+c\\0&1\end{pmatrix}\in N$. 因此 $N<G$. $\forall\begin{pmatrix}a&b\\0&1\end{pmatrix}\in G$，$\begin{pmatrix}1&c\\0&1\end{pmatrix}\in N$，$\begin{pmatrix}a&b\\0&1\end{pmatrix}\begin{pmatrix}1&c\\0&1\end{pmatrix}\begin{pmatrix}a&b\\0&1\end{pmatrix}^{-1}=\begin{pmatrix}a&ac+b\\0&1\end{pmatrix}\begin{pmatrix}\frac{1}{a}&-\frac{b}{a}\\0&1\end{pmatrix}=\begin{pmatrix}1&ac\\0&1\end{pmatrix}\in N$. 所以 $N\lhd G$.

2)　因$\begin{pmatrix}1&0\\0&1\end{pmatrix}\in N_1$，故 $N_1\neq\varnothing$ 且 $N_1\subset N$. $\forall\begin{pmatrix}1&n\\0&1\end{pmatrix},\begin{pmatrix}1&n'\\0&1\end{pmatrix}\in N_1$，$\begin{pmatrix}1&n\\0&1\end{pmatrix}\begin{pmatrix}1&n'\\0&1\end{pmatrix}^{-1}$ $=\begin{pmatrix}1&-n'+n\\0&1\end{pmatrix}\in N_1$，因此 $N_1<N$. $\forall\begin{pmatrix}1&c\\0&1\end{pmatrix}\in N$，$\begin{pmatrix}1&n\\0&1\end{pmatrix}\in N_1$，$\begin{pmatrix}1&c\\0&1\end{pmatrix}\begin{pmatrix}1&n\\0&1\end{pmatrix}\begin{pmatrix}1&c\\0&1\end{pmatrix}^{-1}$ $=\begin{pmatrix}1&n+c\\0&1\end{pmatrix}\begin{pmatrix}1&-c\\0&1\end{pmatrix}=\begin{pmatrix}1&n\\0&1\end{pmatrix}\in N_1$. 所以 $N_1\lhd N$.

3)　取$\begin{pmatrix}1&1\\0&1\end{pmatrix}\in N_1$，$\begin{pmatrix}\frac{1}{2}&1\\0&1\end{pmatrix}\in G$，有$\begin{pmatrix}\frac{1}{2}&1\\0&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}\frac{1}{2}&1\\0&1\end{pmatrix}^{-1}=\begin{pmatrix}\frac{1}{2}&\frac{3}{2}\\0&1\end{pmatrix}\begin{pmatrix}2&-2\\0&1\end{pmatrix}$ $=\begin{pmatrix}1&\frac{1}{2}\\0&1\end{pmatrix}\overline{\in} N_1$. 所以 N_1 不是 G 的不变子群.

注　子群有传递性，但不变子群没有传递性.

6. 一个群 G 的可以写成 $a^{-1}b^{-1}ab$ 形式的元叫做换位子．证明：

(i)　所有的有限个换位子的乘积作成的集合 C 是 G 的一个不变子群；

(ii)　G/C 是交换群；

(iii)　若 N 是 G 的一个不变子群，并且 G/N 是交换群，那么

$$N\supset C.$$

证一　(i)　因 $e=e^{-1}e^{-1}ee\in C$，故 $C\neq\varnothing$ 且 $C\subset G$. 因为有限个换位子的乘积与有限个换位子的乘积的乘积还是有限个换位子的乘积．所以 C 对于 G 的乘法封闭．即 $\forall x_1x_2\cdots x_s,y_1y_2\cdots y_t\in C$，$x_i,y_j(i=1,2,\cdots,s;j=1,2,\cdots,t)$都是换位子，有 $x_1x_2\cdots x_sy_1y_2\cdots y_t\in C$.

又因$(a^{-1}b^{-1}ab)^{-1}=b^{-1}a^{-1}ba$是换位子，故$\forall x_1x_2\cdots x_s\in C$，$x_i(i=1,2,\cdots,s)$是换位子，有$(x_1x_2\cdots x_s)^{-1}=x_s^{-1}x_{s-1}^{-1}\cdots x_1^{-1}\in C$. 所以$C<G$.

$\forall g\in G,c\in C$，有$gcg^{-1}=(gcg^{-1}c^{-1})c\in C$. 所以$C\lhd G$.

称C为G的换位子群.

(ii) $\forall aC,bC\in G/C,aC\cdot bC=abC=ba(a^{-1}b^{-1}ab)C=baC=bC\cdot aC$. 所以$G/C$是交换群.

(iii) $\forall a,b\in G$，因G/N是交换群，故$aN\cdot bN=bN\cdot aN$，即$abN=baN$，于是$ab\in baN$. 因此$\exists n\in N$，使得$ab=ban$，即$a^{-1}b^{-1}ab=n\in N$. 说明G中元的换位子都属于N，又$N<G$，所以N包含任意有限个换位子的乘积，即$C\subset N$.

证二 (i) 见证一.

(ii) $\forall aC,bC\in G/C,(ba)^{-1}(ab)=a^{-1}b^{-1}ab\in C$，从而$ab\sim' ba$[①]，于是$ab$与$ba$属于同一左陪集，即$abC=baC$. 因此$aC\cdot bC=bC\cdot aC$. 所以$G/C$是交换群.

(iii) $\forall a^{-1}b^{-1}ab\in C,a^{-1}b^{-1}abN=a^{-1}b^{-1}N\cdot aN\cdot bN\xlongequal{G/N\text{可换}}a^{-1}b^{-1}N\cdot bN\cdot aN=a^{-1}b^{-1}baN=eN=N$，于是$a^{-1}b^{-1}ab\in N$. 又$N<G$，所以$C\subset N$.

证三 (i) 见证一.

(ii) $\forall aC,bC\in G/C,a^{-1}C\cdot b^{-1}C\cdot aC\cdot bC=a^{-1}b^{-1}abC=C$. 用$a^{-1}C\cdot b^{-1}C$的逆元$(a^{-1}C\cdot b^{-1}C)^{-1}=bC\cdot aC$左乘等式两端，得$aC\cdot bC=bC\cdot aC\cdot C=bC\cdot aC$（因$C$是$G/C$的单位元）. 所以$G/C$是交换群.

(iii) 见证一.

注 1) 用换位子$a^{-1}b^{-1}ab$右乘ba，就调换了b与a的位置，即$ba(a^{-1}b^{-1}ab)=ab$.

2) G的换位子群C实际上是由G中元的所有换位子生成的子群. 即：设$Q=\{G\text{中元的所有换位子}\}$，则$C=(Q)=\left\{q_1q_2\cdots q_s\,\middle|\,q_i\in Q,s\text{是任意正整数}\right\}=\bigcap\limits_{\substack{H<G\\H\supset Q}}H$. 所有换位子未必能作成$G$的一个子群，因为两个换位子的积不一定还是一个换位子.

3) $GL_n(\mathbb{C})$是n次完全线性群，$SL_n(\mathbb{C})$是n次特殊线性群. 与第八章，一，6同理，可知$SL_n(\mathbb{C})\lhd GL_n(\mathbb{C})$且$GL_n(\mathbb{C})/SL_n(\mathbb{C})\cong\mathbb{C}^*$，这里$\mathbb{C}^*$是非零复数集对于普通乘法作成的交换群. 因而$GL_n(\mathbb{C})/SL_n(\mathbb{C})$也是交换群. 由该命题(iii)知，$GL_n(\mathbb{C})$的换位子群包含在$SL_n(\mathbb{C})$中. 实际上，$SL_n(\mathbb{C})$就是$GL_n(\mathbb{C})$的换位子群，证明略.

4) 该命题说明：对于任意群G，总存在一个不变子群C（即换位子群），使G/C为交换群，且换位子群C是G的使商群，G/C为交换群的最小不变子群. 我们知道$G\sim G/C$. 交换群G/C较易于研究，且这里C最小，从而G/C最大. 那么G/C最接近于G，因此利用G/C来研究G的性质较好.

5) G是交换群$\Leftrightarrow G$的换位子群$C=\{e\}$.

证 G是交换群$\Leftrightarrow\forall a,b\in G,ab=ba$

$\Leftrightarrow\forall a,b\in G,a^{-1}b^{-1}ab=e\Leftrightarrow C=\{e\}$.

由此可知，换位子群是测量可换性的尺度.

---

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 67

6）　当 G 是交换群时，G 的换位子群 $C=\{e\}$，因而 $G/C=G/\{e\}=\{\{a\}\mid a\in G\}\cong G$.

7）　设 $H<G$ 且 G 的换位子群 $C\subset H$，则①　$H\lhd G$；②　G/H 是交换群.

证　①　$\forall g\in G,h\in H$，因 $C\subset H$. 又 $ghg^{-1}h^{-1}\in C$，故 $ghg^{-1}h^{-1}\in H$，从而 $ghg^{-1}=(ghg^{-1}h^{-1})h\in H$. 所以 $H\lhd G$.

②　$\forall aH,bH\in G/H,a^{-1}b^{-1}ab\in C\subset H$. 即 $(ba)^{-1}ab\in H$，从而 $abH=baH$，于是 $aH\cdot bH=bH\cdot aH$. 所以 G/H 可换.

该命题 7)是命题 6 中的(i)与(ii)的推广，只需取 $H=C$ 即可.

由该命题 7)可见命题 6 中的(iii)的逆命题也成立.

由该命题 7)还知道：可以用群 G 的换位子群 C 来构造不变子群和交换群．如取 $g\in G$，但 $g\overline{\in} C$，那么由元 g 和 C 的元的全体就生成了一个 G 的不变子群 H，且 G/H 是交换群.

8）　若 $N\lhd G$，N' 是 N 的换位子群，则 $N'\lhd G$.

证　由子群的传递性，$N'<G$. $\forall g\in G,\forall x^{-1}y^{-1}xy\in N',x,y\in N$，

$$
\begin{aligned}
g(x^{-1}y^{-1}xy)g^{-1}&=(gx^{-1}g^{-1})(gy^{-1}g^{-1})(gxg^{-1})(gyg^{-1})\\
&=(gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}).
\end{aligned}
$$

因 $N\lhd G$，故 $gxg^{-1},gyg^{-1}\in N$，从而 $g(x^{-1}y^{-1}xy)g^{-1}$ 是 N 中元的换位子，于是 $g(x^{-1}y^{-1}xy)g^{-1}\in N'$. 同理，$\forall n\in N'$，也有 $gng^{-1}\in N'$. 所以 $N'\lhd G$.

我们知道，一般不变子群不可传递，但当 $N'\lhd N$，$N\lhd G$，其中 N' 是 N 的换位子群时，有可传性，即 $N'\lhd G$.

7. 我们看一个集合 A 到集合 $\bar{a}$ 的满射 ϕ．证明：若 A 的子集 S 是 $\bar{a}$ 的子集 $\bar{S}$ 的逆象，$\bar{S}$ 一定是 S 的象；但若 $\bar{S}$ 是 S 的象，S 不一定是 $\bar{S}$ 的逆象.

证　1）　$\bar{S}$ 是 S 在满射 ϕ 下的象．事实上，已知 $S=\{a\mid\phi(a)=\bar{a},\bar{a}\in\bar{S}\}$. 要证 $\bar{S}=\{\bar{a}\mid\phi(a)=\bar{a},a\in S\}$. $\forall\bar{s}\in\bar{S}$，因 $\bar{S}$ 的逆象是 S，故 $\bar{S}$ 中每个元的逆象都在 S 中，从而 $\exists s\in S$，使得 $\phi(s)=\bar{s}$，于是 $\bar{s}\in\{\bar{a}\mid\phi(a)=\bar{a},a\in S\}$. 反之，$\forall\bar{s}\in\{\bar{a}\mid\phi(a)=\bar{a},a\in S\}$，都 $\exists s\in S$，使得 $\phi(s)=\bar{s}$．因 S 是 $\bar{S}$ 的逆象，故 S 中每个元的象都在 $\bar{S}$ 中，于是 $\bar{s}\in\bar{S}$. 所以 $\bar{S}=\{\bar{a}\mid\phi(a)=\bar{a},a\in S\}$.

2）　S 不一定是 $\bar{S}$ 的逆象.

例　设 $A=\{a,b\}$，$\bar{A}=\{c\}$. $\phi:a\to c,b\to c$ 是 A 到 $\bar{A}$ 的一个满射．令 $S=\{a\}$，于是 $\bar{S}=\{c\}$ 是 S 的象．但 $S=\{a\}$ 不是 $\bar{S}=\{c\}$ 的逆象 $\{a,b\}$. 问题关键在于 ϕ 不是单射，$\bar{S}$ 中的元的逆象不唯一，有的逆象就未必属于 S.

又例　$\mathbb{C}$ 是复数集，$\mathbb{R}$ 是实数集．$\phi:\alpha\to|\alpha|$ 是 $\mathbb{C}$ 到 $\mathbb{R}$ 的一个满射．取 $S=\{bi\mid b\in\mathbb{R}\}\subset\mathbb{C}$，于是 S 在 ϕ 下的象是全体非负实数集 $\bar{S}$. 但 $\bar{S}$ 的逆象是 $\mathbb{C}\neq S$，从而 $\mathbb{C}$ 的子集 S 的象 $\bar{S}$ 的逆象 $\mathbb{C}$ 包含 S，但不等于 S.

注　设 ϕ 是群 G 到群 $\bar{G}$ 的一个同态满射，$H<G$. 又设 $\bar{H}$ 是 H 在 ϕ 下的象，记为 $\phi(H)=\bar{H}$. 记 $\bar{H}$ 在 ϕ 下的逆象为 $\phi^{-1}(\bar{H})=\phi^{-1}(\phi(H))$. 则

1）　$\phi^{-1}(\phi(H))$ 未必是 H.

2）　$\phi^{-1}(\phi(H))=HK$，这里 $K=\ker\phi$.

3）　当 $H\supset K=\ker\phi$ 时，有 $\phi^{-1}(\phi(H))=H$. 反之，也成立.

4) 若$\forall a\in G$,有$\phi^{-1}(\phi(a))=aK$,这里$K=\ker\phi$.

证 1) 例,取$G=$整数加群$\mathbb{Z}$,$\overline{G}=\{\overline{e}\}$单元群.设$n$是大于1的一个固定整数,取$H=\{nq\mid q\in\mathbb{Z}\}$,则$H<G$. $\phi:x\to\overline{e}$是G到$\overline{G}$的一个同态满射.于是$\phi^{-1}(\phi(H))=\phi^{-1}(\overline{e})=G\neq H$.

2) $\forall x\in\phi^{-1}(\phi(H))$,即$x$是$\phi(H)$中一个元的逆象,从而$\phi(x)\in\phi(H)$,因此$\exists h\in H$,使得$\phi(x)=\phi(h)$,于是$\phi(h^{-1}x)=\phi(h^{-1})\phi(x)=\phi(h)^{-1}\phi(x)=\phi(h)^{-1}\phi(h)=\overline{e}$,这里$\overline{e}$是$\overline{G}$的单位元.所以$h^{-1}x\in K$.即$\exists k\in K$,使得$h^{-1}x=k$,从而$x=hk\in HK$,于是$\phi^{-1}(\phi(H))\subset HK$.另一方面,$\forall hk\in HK$,这里$h\in H,k\in K$,$\phi(hk)=\phi(h)\phi(k)=\phi(h)\overline{e}=\phi(h)\in\phi(H)$,从而$hk$是$\phi(H)$中一个元的逆象,即$hk\in\phi^{-1}(\phi(H))$,于是$HK\subset\phi^{-1}(\phi(H))$.所以$\phi^{-1}(\phi(H))=HK$.

3) 当$H\supset K$时,因$H<G,K<G$,故$\phi^{-1}(\phi(H))=HK=H$.反之,若$\phi^{-1}(\phi(H))=H$,由2),$H=HK$,则显然$K\subset H$.

4) 用与2)的同样的证法可得结论.

8. 假定群G与群$\overline{G}$同态,$\overline{N}$是$\overline{G}$的一个不变子群,N是$\overline{N}$的逆象.证明:$G/N\cong\overline{G}/\overline{N}$.

证一 由同态基本定理[①],只需证:1)$G\sim\overline{G}/\overline{N}$;2)$N$是$G$到$\overline{G}/\overline{N}$的一个同态满射的核.

1) 由已知,可设$\phi:x\to\overline{x}=\phi(x)$是$G$到$\overline{G}$的一个同态满射.则$\phi_o:\overline{x}\to\overline{x}\,\overline{N}=\phi_o(\overline{x})$是$\overline{G}$到$\overline{G}/\overline{N}$的一个同态满射[②].由第二章,二,5,$\phi':x\to\overline{x}\,\overline{N}=\phi_o(\phi(x))$是$G$到$\overline{G}/\overline{N}$的一个同态满射.所以$G\overset{\phi'}{\sim}\overline{G}/\overline{N}$.

2) 下面证明$N=\ker\phi'$,其中N是$\overline{N}$在ϕ下的逆象.$\forall x\in N$,下面证$x\in\ker\phi'$. $\phi'(x)=\phi_0(\phi(x))=\phi_0(\overline{x})=\overline{x}\,\overline{N}$,其中$\phi(x)=\overline{x}$.因$N$是$\overline{N}$在$\phi$下的逆象,故由第八章,二,7,$\overline{N}$是$N$在$\phi$下的象.所以$\phi(x)=\overline{x}\in\overline{N}$,于是$\phi'(x)=\overline{x}\,\overline{N}=\overline{N}$,而$\overline{N}$是$\overline{G}/\overline{N}$的单位元,因此$x\in\ker\phi'$.另一方面,$\forall x\in\ker\phi'$,有$\phi'(x)=\overline{N}$,其中$\overline{N}$是$\overline{G}/\overline{N}$的单位元,下面证$x\in N$.因$\phi'(x)=\phi_O(\phi(x))=\phi_O(\overline{x})=\overline{x}\,\overline{N}$,其中$\phi(x)=\overline{x}$,故$\overline{N}=\overline{x}\,\overline{N}$.于是$\overline{x}\in\overline{N}$,其中$\phi(x)=\overline{x}$.因$\overline{N}$在$\phi$下的逆象是$N$,故$x\in N$.综上,$N=\ker\phi'$.所以由同态基本定理,$G/N\cong\overline{G}/\overline{N}$.

证二 因$\overline{N}\lhd\overline{G}$,故$\overline{G}/\overline{N}$是商群.设$\phi$是$G$到$\overline{G}$的同态满射,又$N$是不变子群$\overline{N}$在$\phi$下的逆象,从而$N\lhd G$[③].所以$G/N$是商群.$\forall Na\in G/N$,令

$$\psi:Na\to\overline{N}\overline{a},\ \text{而}\ \overline{a}=\phi(a)\in\overline{G}.$$

则ψ是G/N与$\overline{G}/\overline{N}$间的一个同构映射.事实上,

1) $\forall Na\in G/N$,因ϕ是映射,故$\exists\overline{a}\in\overline{G}$,使得$\phi(a)=\overline{a}$,从而$\exists\overline{N}\overline{a}\in\overline{G}/\overline{N}$,使得$\psi:Na\to\overline{N}\overline{a}$,又这样的$\overline{N}\overline{a}$唯一.因为:若$Na=Nb$,则$a\sim b$,即$ab^{-1}\in N$.因$N$是$\overline{N}$在$\phi$下的

---

① 张禾瑞.近世代数基础.北京:高等教育出版社,1978.76.定理2.

② 同上.75.定理1.

③ 同上.78.定理4.

逆象，故 $\overline{N}$ 是 N 在ϕ下的象，从而$\phi(ab^{-1})=\phi(a)\phi(b)^{-1}\in\overline{N}$. 于是$\phi(a)=\bar{a}\sim\phi(b)=\bar{b}$. 因此 $\overline{N}\bar{a}=\overline{N}\bar{b}$. 可见 G/N 的每一个元 Na 在 ψ 下有且只有一个象 $\overline{N}\bar{a}\in\overline{G}/\overline{N}$. 所以 ψ 是映射.

2)　$\forall\ \overline{N}\bar{a}\in\overline{G}/\overline{N}$，因$\phi$是满射，故 $\exists\ a\in G$，使得 $\bar{a}=\phi(a)$，从而 $\exists\ Na\in G/N$，使得 ψ: $Na\rightarrow\overline{N}\bar{a}$. 所以 ψ 是满射.

3)　若 $\overline{N}\bar{a}=\overline{N}\bar{b}$，则 $\bar{a}\sim\bar{b}$，即 $\bar{a}\,\bar{b}^{-1}\in\overline{N}$，从而$\phi(ab^{-1})=\phi(a)\phi(b)^{-1}=\bar{a}\,\bar{b}^{-1}\in\overline{N}$. 因 $\overline{N}$ 在ϕ下的逆象是 N，故 $ab^{-1}\in N$，即 $a\sim b$，于是 $Na=Nb$. 所以 ψ 是单射.

4)　$\forall\ Na,Nb\in G/N$.

$$\psi: Na\rightarrow\overline{N}\bar{a},\ \text{而}\ \bar{a}=\phi(a),$$
$$Nb\rightarrow\overline{N}\bar{b},\ \text{而}\ \bar{b}=\phi(b).$$

于是

$$\psi: Na\cdot Nb=Nab\rightarrow\overline{N}\,\overline{ab}=\overline{N}\bar{a}\,\bar{b}=\overline{N}\bar{a}\cdot\overline{N}\bar{b}.$$

所以 ψ 是G/N 与 $\overline{G}/\overline{N}$ 间的一个同构映射．即 $G/N\overset{\psi}{\cong}\overline{G}/\overline{N}$.

例　设 $G=(a)$是 12 阶循环群，$\overline{G}=(b)$是 6 阶循环群．令

$$\phi(e)=\phi(a^6)=\bar{e},\ \phi(a)=\phi(a^7)=b,$$
$$\phi(a^2)=\phi(a^8)=b^2,\ \phi(a^3)=\phi(a^9)=b^3,$$
$$\phi(a^4)=\phi(a^{10})=b^4,\ \phi(a^5)=\phi(a^{11})=b^5.$$

则ϕ是 G 到 $\overline{G}$ 的一个同态满射．取 $\overline{N}=\{\bar{e},b^3\}=(b^3)\lhd\overline{G}$，于是 $\overline{N}$ 在ϕ下的逆象 $N=\{e,a^3,a^6,a^9\}=(a^3)$. 由该命题，$G/(a^3)\cong\overline{G}/(b^3)$.

注　1)　该命题表示两个同态群的商群之间的一个同构关系．它是同态基本定理的推广．事实上，设ϕ是群 G 到群 $\overline{G}$ 的一个同态满射．取 $\overline{N}=\{\bar{e}\}$，其中 $\bar{e}$ 是 $\overline{G}$ 的单位元．显然 $\overline{N}\lhd\overline{G}$ 且$\overline{G}/\overline{N}\cong\overline{G}$. 则 $\overline{N}$ 在 ϕ 下 的 逆 象 $N=\ker\phi$. 由 该 命 题：$G/N\cong\overline{G}/\overline{N}$，即 $G/N\cong\overline{G}$.

2)　将该命题的条件改为："设ϕ是群 G 到群 $\overline{G}$ 的一个同态满射，$N\lhd G$，$\overline{N}$ 是 N 在ϕ下的象"，于是该命题的结论："$G/N\cong\overline{G}/\overline{N}$"未必成立．因为在这个条件下，由第八章，二，7，注，$\overline{N}$ 的逆象是 NK，其中 $K=\ker\phi$．所以结论应为 $G/NK\cong\overline{G}/\overline{N}$.

我们再举出一个例子．设 $G=\mathbf{Z}_{12}$，$\overline{G}=\mathbf{Z}_6$，则$\phi$：$[a]\rightarrow[a]$是 $\mathbf{Z}_{12}$ 到 $\mathbf{Z}_6$ 的一个同态满射. $\ker\phi=K=\{[0],[6]\}$．取 $N=\{[0],[4],[8]\}$，则 $N\lhd\mathbf{Z}_{12}$. N 在ϕ下的象 $\overline{N}=\phi(N)=\{\phi([0]),\phi([4]),\phi([18])\}=\{[0],[4],[2]\}$. 于是 $\mathbf{Z}_{12}$ 关于N的商群 $\mathbf{Z}_{12}/N=\{N,[1]+N,[2]+N,[3]+N\}=\{\{[0],[4],[8]\},\{[1],[5],[9]\},\{[2],[6],[10]\},\{[3],[7],[11]\}\}$. $\mathbf{Z}_6$ 关于 $\overline{N}$ 的商群 $\mathbf{Z}_6/\overline{N}=\{\overline{N},[1]+\overline{N}\}=\{\{[0],[2],[4]\},\{[1],[3],[5]\}\}$. 显然 $\mathbf{Z}_{12}/N$ 与 $\mathbf{Z}_6/\overline{N}$不同构．问题产生在 N 不包含 $K=\ker\phi$，但 $N+K=\{[0],[2],[4],[6],[8],[10]\}$. $\mathbf{Z}_{12}/N+K=\{N+K,[1]+N+K\}$，从而 $\mathbf{Z}_{12}/N+K\cong\mathbf{Z}_6/\overline{N}$.

9. 假定G和$\overline{G}$是两个有限循环群，它们的阶各是m和n. 证明：G和$\overline{G}$同态，当且仅当$n|m$时.

证一　(⇒)　设$G\overset{\phi}{\sim}\overline{G}$，$N=\ker\phi$，则由同态基本定理，$G/H\cong\overline{G}$. 从而$|G/N|=|\overline{G}|$，即$\dfrac{|G|}{|N|}=|\overline{G}|$，于是 $m=|N|\cdot n$. 所以 $n|m$.

($\Leftarrow$) 设 $G=(a)$，$\overline{G}=(\bar{a})$，则 $\phi: a^i \rightarrow \bar{a}^i$ 是 G 到 $\overline{G}$ 的一个同态满射．事实上，

1) $\forall a^i \in G$，$\exists \bar{a}^i \in \overline{G}$，使得 $\phi(a^i)=\bar{a}^i$．若 $a^i=a^j$，则 $a^{i-j}=e$，因 $|a|=m$，故 $m \mid i-j$．又 $n \mid m$，从而 $n \mid i-j$．因 $|\bar{a}|=n$，故 $\bar{a}^{i-j}=\bar{e}$，于是 $\bar{a}^i=\bar{a}^j$，即对于 G 中的每一个元，不论其表法如何，在 ϕ 下有且只有唯一的一个象．所以 ϕ 是映射.

2) $\forall \bar{a}^k \in \overline{G}$，$\exists a^k \in G$，使得 $\phi(a^k)=\bar{a}^k$．所以 ϕ 是满射.

3) $\forall a^i, a^j \in G$，$\phi(a^i a^j)=\phi(a^{i+j})=\bar{a}^{i+j}=\bar{a}^i \bar{a}^j=\phi(a^i)\phi(a^j)$.

综上，ϕ 是 G 到 $\overline{G}$ 的一个同态满射．所以 $G \overset{\phi}{\sim} \overline{G}$.

证二 ($\Rightarrow$) 已知 $G \overset{\phi}{\sim} \overline{G}$，由第六章，二，7，同态满射 ϕ 把 G 的生成元 a 映到 $\overline{G}$ 的生成元 $\bar{a}$，即 $\phi: a \rightarrow \bar{a}$．由 $|a|=m$ 及 ϕ 保持运算，有 $\phi: a^m=e \rightarrow \bar{a}^m$．在同态满射 ϕ 下，G 的单位元 e 的象是 $\overline{G}$ 的单位元 $\bar{e}$，即 $\phi: e \rightarrow \bar{e}$①．由 ϕ 是映射，$\bar{a}^m=\bar{e}$，又 $|\bar{a}|=n$，从而 $n \mid m$.

($\Leftarrow$) 设 $G=(a)$，$\overline{G}=(\bar{a})$，则 $\phi: a^i \rightarrow \bar{a}^r$，其中 $i=qn+r, 0 \leqslant r<n$，是 G 到 $\overline{G}$ 的一个同态满射．事实上，

1) $\forall a^i \in G$，$\exists q, r \in \mathbb{Z}$，使得 $i=qn+r, 0 \leqslant r<n$，从而 $\exists \bar{a}^r \in \overline{G}$，使得 $\phi(a^i)=\bar{a}^r$，且这样的 r 唯一．即设 $a^i=a^j, i \neq j, i=q_1 n+r_1, j=q_2 n+r_2, 0 \leqslant r_1<n, 0 \leqslant r_2<n, \phi(a^i)=\bar{a}^{r_1}$，$\phi(a^j)=\bar{a}^{r_2}$，则 $r_1=r_2$．不然，若 $r_1 \neq r_2$，不妨设 $r_1>r_2$，则 $i-j=(q_1-q_2)n+(r_1-r_2), 0<r_1-r_2<n$．因 $a^{i-j}=e, |a|=m$，故 $m \mid i-j$．又 $n \mid m$，从而 $n \mid i-j$．显然 $n \mid (q_1-q_2)n$，可见 $n \mid r_1-r_2$，此与 $0<r_1-r_2<n$ 矛盾．所以 $r_1=r_2$．当然 $\bar{a}^{r_1}=\bar{a}^{r_2}$，于是 ϕ 是映射.

2) $\forall \bar{a}^r \in \overline{G}, 0 \leqslant r<n$，$\exists a^r \in G$，使得 $\phi(a^r)=\bar{a}^r$，其中 $r=0n+r, 0 \leqslant r<n$．于是 ϕ 是满射.

3) $\forall a^h, a^k \in G$，设 $h=q'n+r', 0 \leqslant r'<n, k=q''n+r'', 0 \leqslant r''<n$，则 $\phi(a^h)=\bar{a}^{r_1}$，$\phi(a^k)=\bar{a}^{r''}$，$h+k=(q'+q'')n+r'+r''$．设 $r'+r''=qn+r, 0 \leqslant r<n$，则 $h+k=(q'+q''+q)n+r$．于是 $\phi(a^h a^k)=\phi(a^{h+k})=\bar{a}^r=\bar{a}^{r'+r''-nq}=\bar{a}^{r'+r''}(\bar{a}^n)^{-q} \xlongequal{\text{由}|a|=n} \bar{a}^{r'}\bar{a}^{r''}=\phi(a^h)\phi(a^k)$.

所以 $G \overset{\phi}{\sim} \overline{G}$.

证三 ($\Rightarrow$) 见证一.

($\Leftarrow$) 设 $G=(a)$．因 $n \mid m$，故 $(n,m)=n$．由第六章，二，5，$|a^n|=\dfrac{m}{(n,m)}=\dfrac{m}{n}$．于是 $N=(a^n)$ 是 G 的 $\dfrac{m}{n}$ 阶不变子群．所以 $G \sim G/N$．因 G 是循环群，由第六章，二，7，G/N 也是循环群．又 $|G/N|=\dfrac{m}{\frac{m}{n}}=n$，$\overline{G}$ 也是 n 阶循环群，故由第六章，一，4 中结论，$G/N \cong \overline{G}$，再由第二章，二，5，$G \sim \overline{G}$.

注 若 G 与 $\overline{G}$ 不是循环群，则该命题的必要性也成立．即设 G 和 $\overline{G}$ 是两个有限群，且 $|G|=m$，$|\overline{G}|=n$．若 $G \sim \overline{G}$，则 $n \mid m$.

10. 假定 G 是一个循环群，N 是 G 的一个子群．证明：G/N 也是循环群.

---

① 张禾瑞．近世代数基础．北京：高等教育出版社，1978. 43. 定理 2.

证一 设 $G=(a)$. 由第六章,二,4,G 是交换群. 于是 $N\lhd G$①,从而 G/N 是商群. 因此 $G\sim G/N$. 由第六章,二,7,G/N 也是循环群.

证二 设 $G=(a)$,由第六章,二,4,G 是交换群. 于是 $N\lhd G$②,从而 G/N 是商群.

$\forall bN\in G/N, b\in G$,可设 $b=a^k, k\in\mathbb{Z}$,从而 $bN=a^kN$. 我们有 $a^kN=(aN)^k$. 事实上,

1) k 是正整数时,由商群 G/N 中元的乘法定义:$xN\cdot yN=xyN$,有

$$(aN)^k=\overbrace{aN\cdot aN\cdots aN}^{k\text{个}}=(\overbrace{a\,a\quad\cdots\quad a}^{k\text{个}})N=a^kN.$$

2) $k=0$ 时,

$$(aN)^k=(aN)^0=N=eN=a^0N=a^kN.$$

3) k 是负整数时,设 $k=-h$,h 是正整数,$(aN)^k=(aN)^{-h}=((aN)^{-1})^h=(a^{-1}N)^h=(a^{-1})^hN=a^{-h}N=a^kN$.

所以 $bN=(aN)^k$,于是 $G/N=(aN)$ 是循环群.

注 1) 循环群 $G=(a)$ 的商群 G/N 的生成元是 G 的生成元 a 所在的 N 的陪集 aN.

例 取 $G=\mathbb{Z}_{12}=([1])$,$N=([6])=\{[0],[6]\}\lhd\mathbb{Z}_{12}$. 则 $\mathbb{Z}_{12}/([6])=([1]+N)=\{[0]+N,[1]+N,[2]+N,[3]+N,[4]+N,[5]+N\}$,其中 $[0]+N=\{[0],[6]\}$,$[1]+N=\{[1],[7]\}$,$[2]+N=\{[2],[8]\}$,$[3]+N=\{[3]+[9]\}$,$[4]+N=\{[4]+[10]\}$,$[5]+N=\{[5],[11]\}$.

2) 设 $G=(a)$ 是无限循环群,$N=(a^m)\lhd G$ 且 $N\neq\{e\}$,m 是正整数,则 $|G/N|=m$.

证 因 $G/N=(aN)$,故只需证 $|aN|=m$. 事实上,因 $a^m\in N$,故 $(aN)^m=a^mN=N$,而 N 是 G/N 的单位元. $\forall m', 1\leqslant m'<m$,有 $(aN)^{m'}=a^{m'}N\neq N$,不然,若 $a^{m'}N=N$,则 $a^{m'}\in N$,又 $1\leqslant m'<m$. 但由 G 是无限循环群及第七章,二,3 的证明知,m 是 N 中元的唯一确定的最小正整数指数,因此产生了矛盾. 所以 $(aN)^{m'}\neq N$,从而 $|aN|=m$. 于是 $|G/N|=m$.

由第七章,三,2,2)也可知此结论.

读者可进一步考虑:当 G 是有限循环群时,结论是否仍成立.

3) 该命题的逆命题不成立. 即:设 $N\lhd G$,商群 G/N 是循环群,但 G 未必是循环群.

例 取 $G=S_3$,$N=\{(1),(1\ 2\ 3),(1\ 3\ 2)\}<S_3$,因 $[G:N]=\dfrac{|S_3|}{|N|}=\dfrac{6}{3}=2$,故由第八章,二,3,$N\lhd S_3$. 又 $|S_3/N|=2$,而 2 是素数,从而由第七章,二,6,S_3/N 是循环群. 但 S_3 不是循环群.

三、讲与练

1. 设 $GL_n(\mathbf{R})$ 是完全线性群. 试分别验证:

---

①② 张禾瑞. 近世代数基础. 北京:高等教育出版社,1978.71. 例 3.

$$H_1=\left\{(a_{ij})\in GL_n(\mathbf{R})\,\middle|\,a_{ii}=a;\text{当 } i\neq j \text{ 时},a_{ij}=0\right\},$$

$$H_2=\left\{(a_{ij})\in GL_n(\mathbf{R})\,\middle|\,\text{当 } i\neq j \text{ 时},a_{ij}=0\right\},$$

$$H_3=\left\{(a_{ij})\in GL_n(\mathbf{R})\,\middle|\,\text{当 } i>j \text{ 时},a_{ij}=0\right\}$$

是否为 $GL_n(\mathbf{R})$的不变子群.

解 显然 $H_k<GL_n(\mathbf{R})$,$k=1,2,3$. H_1 中每一元都是 n 阶纯量矩阵,而 n 阶纯量矩阵与任一 n 阶矩阵可交换,所以 $H_1\lhd GL_n(\mathbf{R})$.

取 $\begin{pmatrix}1&1&&&\\&1&&&\\&&1&&\\&&&\ddots&\\&&&&1\end{pmatrix}\in GL_n(\mathbf{R})$, $\begin{pmatrix}1&&&&\\&-1&&&\\&&1&&\\&&&\ddots&\\&&&&1\end{pmatrix}\in H_2$,因

$$\begin{pmatrix}1&1&&&\\&1&&&\\&&1&&\\&&&\ddots&\\&&&&1\end{pmatrix}\begin{pmatrix}1&&&&\\&-1&&&\\&&1&&\\&&&\ddots&\\&&&&1\end{pmatrix}\begin{pmatrix}1&1&&&\\&1&&&\\&&1&&\\&&&\ddots&\\&&&&1\end{pmatrix}^{-1}=\begin{pmatrix}1&-2&&&\\&-1&&&\\&&1&&\\&&&\ddots&\\&&&&1\end{pmatrix}\overline{\in}H_2.$$

故 H_2 不是 $GL_n(\mathbf{R})$的不变子群.

取 $\begin{pmatrix}1&&&&\\1&1&&&\\&&1&&\\&&&\ddots&\\&&&&1\end{pmatrix}\in GL_n(\mathbf{R})$, $\begin{pmatrix}1&1&&&\\&1&&&\\&&1&&\\&&&\ddots&\\&&&&1\end{pmatrix}\in H_3$,因

$$\begin{pmatrix}1&&&&\\1&1&&&\\&&1&&\\&&&\ddots&\\&&&&1\end{pmatrix}\begin{pmatrix}1&1&&&\\&1&&&\\&&1&&\\&&&\ddots&\\&&&&1\end{pmatrix}\begin{pmatrix}1&&&&\\1&1&&&\\&&1&&\\&&&\ddots&\\&&&&1\end{pmatrix}^{-1}=\begin{pmatrix}0&1&&&\\-1&2&&&\\&&1&&\\&&&\ddots&\\&&&&1\end{pmatrix}\overline{\in}H_3,$$

故 H_3 不是 $GL_n(\mathbf{R})$的不变子群.(以上各矩阵,除主对线以外的没有注明的元素都是 0.)

2. 下面关于不变子群的一些叙述,哪些是正确的?

1) 循环群的子群都是不变子群.

2) 若群 G 的子群 H 的每个左陪集 aH 的元的个数与 H 的元的个数相同,则 $H\lhd G$.

3) 群 G 的不变子群是交换群.

4) 群 G 的交换子群是 G 的不变子群.

5) 设 $N\lhd G$,$N\subset H<G$,则 $N\lhd H$.

6) 设 H 是群 G 的一个阶为 n 的子群,且 G 中只有这样唯一的一个 n 阶子群,则 $H\lhd G$.

7) 设 $N\lhd G$,$H<G$ 且 $H\cong N$,则 $H\lhd G$.

解 1) 正确. 因为循环群是交换群.

2）不正确．例，$H=\{(1),(12)\}<S_3$. $\forall a\in G, aH$ 的元的个数$=|H|=2$，但 H 不是 S_3 的不变子群.

3）不正确．非交换群 G 就是 G 的一个不变子群.

4）不正确．例，$H=\{(1),(12)\}$是 S_3 的交换子群，但 H 不是 S_3 的不变子群.

5）正确．证：$N<H$. 事实上，$N\subset H$. 已知 $N<G$，从而 $N\neq\varnothing$. (i) 因 $H<G$，故 H 的乘法就是 G 的乘法．因 $N<G$，故 N 对于 G 的乘法封闭，从而 N 对于 H 的乘法也封闭．(ii) $\forall n\in N$，因 $N<G$，故 n 在 G 里的逆元 $n^{-1}\in N$，又 $H<G$，从而 $n(\in N\subset H)$在 G 里的逆元 n^{-1}就是 n 在 H 里的逆元，于是 n 在 H 里的逆元 $n^{-1}\in N$. 所以 $N<H$. $\forall h\in H\subset G$，$\forall n\in N$，因 $N\lhd G$，故 $hnh^{-1}\in N$. 所以 $N\lhd H$.

注　①　命题说明：若 $N\lhd G$，则 N 也是"中间子群"H 的不变子群.

②　设 $N\lhd G, N\subset H<G$，但未必 $H\lhd G$. 例，$B_4=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}\lhd S_4$. $\{(1),(1\ 2)\}<S_4$，由第八章，二，4，$B_4\{(1),(1\ 2)\}=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3),(1\ 2),(3\ 4),(1\ 2\ 3\ 4),(1\ 4\ 3\ 2)\}<S_4$. $B_4\subset B_4\{(1),(1\ 2)\}$. 但 $B_4\{(1),(1\ 2)\}$ 不是 S_4 的不变子群，因为取$(1\ 3)\in S_4$，$(1\ 2)\in B_4\{(1),(1\ 2)\}$，有$(1\ 3)(1\ 2)(1\ 3)^{-1}=(2\ 3)\overline{\in} B_4\{(1),(1\ 2)\}$.

6）正确．证：$\forall a\in G, aHa^{-1}<G$. 事实上，因 $e=aea^{-1}\in aHa^{-1}$，故 $aHa^{-1}\neq\varnothing$ 且 $aHa^{-1}\subset G$. $\forall ah_1a^{-1}, ah_2a^{-1}\in aHa^{-1}$，$(ah_1a^{-1})(ah_2a^{-1})^{-1}=ah_1a^{-1}ah_2^{-1}a^{-1}=ah_1h_2a^{-1}\in aHa^{-1}$. 所以 $aHa^{-1}<G$. 由第八章，一，7，aHa^{-1}是 H 的任一共轭子群．因$\phi: h\to aha^{-1}$是 H 与 aHa^{-1}间的一个一一映射，故$|aHa^{-1}|=|H|=n$. 由题设中的唯一性，$aHa^{-1}=H$，$\forall a\in G$. 所以 $H\lhd G$.

7）不正确．例，$B_4=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}\lhd S_4$，$H=\big(\{(1\ 2),(3\ 4)\}\big)=\big\{(1),(1\ 2),(3\ 4),(1\ 2)(3\ 4)\big\}<S_4$. 又

$$\begin{aligned}\phi:(1)&\to(1)\\(1\ 2)&\to(1\ 2)(3\ 4)\\(3\ 4)&\to(1\ 3)(2\ 4)\\(1\ 2)(3\ 4)&\to(1\ 4)(2\ 3)\end{aligned}$$

是 H 与 B_4 间的一个同构映射，从而 $H\cong B_4$. 但 H 不是 S_4 的不变子群，因取$(1\ 3\ 4)\in S_4$，$(1\ 2)\in H$，有$(1\ 3\ 4)(1\ 2)(1\ 3\ 4)^{-1}=(2\ 4)\overline{\in} H$.

3. 下面关于群的中心的叙述，哪些是正确的？

1）G 是交换群 $\Leftrightarrow G$ 的中心 $Z=G$.

2）若一个群 G 的中心 Z 不是整个群 G，则 G 不能是循环群.

3）任何群 G 的元的个数永远是这个群 G 的中心的元的个数的倍数.

4）群的每一个交换子群都是群的中心.

5）若一个群 G 不是交换的，则 G 中必至少有两个元不在 G 的中心 Z 里.

6）群的中心是交换群.

7）若群 G 的中心只含 G 的单位元 e，那么 G 必为非交换群.

8）设 Z 是群 G 的中心，$Z_1<Z$，则 $Z_1\lhd G$.

9）设群 $G\overset{\phi}{\sim}\overline{G}$，$Z$ 是 G 的中心，$\overline{Z}$ 是 $\overline{G}$ 的中心，则 $\forall a\in Z, \phi(a)\in\overline{Z}$.

解 1) 正确．证：G是交换群$\Leftrightarrow G\subset Z$，又$Z\subset G\Leftrightarrow Z=G$.

2) 正确．证：$Z\neq G\Rightarrow G$不是交换群$\Rightarrow G$不是循环群.

3) 不正确．因为当$|G|=\infty$时，命题不成立．当$|G|$有限时，命题成立.

4) 不正确．例，$H=\{(1),(1\ 2)\}$是S_3的交换子群，但H不是S_3的中心$\{(1)\}$.

5) 正确．证：因G不是交换群，故$\exists a,b\in G, a\neq b$，使得$ab\neq ba$. 从而$a\overline{\in} Z, b\overline{\in} Z$.

6) 正确．由定义直接可知.

7) 不正确．当$G=\{e\}$时，G是交换群．当$G\neq\{e\}$时，G是非交换群.

8) 正确．证：因$Z_1<Z$，又$Z<G$，故$Z_1<G$. $\forall g\in G, y\in Z_1\subset Z$，因$Z$是$G$的中心，故$gz=zg$，从而$gzg^{-1}=zgg^{-1}=z\in Z_1$. 所以$Z_1\lhd G$.

9) 正确．证：$\forall a\in Z, \phi(a)\in\overline{G}$. 下面证$\phi(a)\in\overline{Z}$. $\forall\overline{x}\in\overline{G}$，因$\phi$是满射，故$\exists x\in G$，使得$\phi(x)=\overline{x}$. 因$a\in Z$，故$ax=xa$. 因$\phi$是同态映射，故$\phi(a)\overline{x}=\phi(a)\phi(x)=\phi(ax)=\phi(xa)=\phi(x)\phi(a)=\overline{x}\,\phi(a)$. 所以$\phi(a)\in\overline{Z}$.

注 设群$G\overset{\phi}{\sim}\overline{G}$，$Z$与$\overline{Z}$分别是$G$与$\overline{G}$的中心，$a\in G, \phi(a)\in\overline{Z}$，但未必$a\in Z$. 例，$\phi: A\rightarrow|A|$是实数域$\mathbb{R}$上2阶线性群$GL_2(\mathbb{R})$到非零实数乘群$\mathbb{R}^*$的一个同态满射．因$\mathbb{R}^*$是交换群，故$\mathbb{R}^*$的中心是$\mathbb{R}^*$．因$GL_2(\mathbb{R})$不是交换群，故$GL_2(\mathbb{R})$的中心$Z$不是$GL_2(\mathbb{R})$. $\exists\begin{pmatrix}0&1\\1&1\end{pmatrix}\in GL_2(\mathbb{R})$，$\begin{pmatrix}0&1\\1&1\end{pmatrix}\overline{\in} Z$，而$\phi\left(\begin{pmatrix}0&1\\1&1\end{pmatrix}\right)=\begin{vmatrix}0&1\\1&1\end{vmatrix}=-1\in\mathbb{R}^*$.

4. 1) 证明：有限群G的商群G/N一定是有限群．反之，群G的商群G/N有限时，G一定是有限群吗？

2) 证明：交换群G的商群G/N一定是交换群．反之，群G的商群G/N是交换群时，G一定是交换群吗？

证 1) 因G是有限群，又$N<G$，故N也是有限群．而G/N的阶是N在G里的指数，因此$|G/N|=[G:N]=\dfrac{|G|}{|N|}$，从而$G/N$是有限群．反之，$G$的商群$G/N$有限时，$G$未必是有限群．例，整数加群$\mathbb{Z}$的商群$\mathbb{Z}/(n)=\mathbb{Z}_n$是模$n$的剩余类加群，因此商群$\mathbb{Z}/(n)$是$n$阶有限群．但$\mathbb{Z}$是无限群.

2) $\forall Ng_1, Ng_2\in G/N$，因$G$是交换群，故$g_1g_2=g_2g_1$，从而$Ng_1\cdot Ng_2=Ng_1g_2=Ng_2g_1=Ng_2\cdot Ng_1$. 所以$G/N$是交换群(或我们有$G\sim G/N$，因$G$是交换群，故$G/N$也是交换群)．反之，$G$的商群$G/N$是交换群时，$G$未必是交换群．例，$N=\{(1),(123),(1\ 3\ 2)\}\lhd S_3$，$S_3$的商群$S_3/N=\{N,(1\ 2)N\}$是2阶交换群，但$S_3$不是交换群.

5. 设G是有限群，且$G\overset{\phi}{\sim}\overline{G}$，证明：$\overline{G}$是有限群，且$|\overline{G}|\,\big|\,|G|$.

证 由同态基本定理，$G/\ker\phi\cong\overline{G}$，从而$|\overline{G}|=|G/\ker\phi|=\dfrac{|G|}{|\ker\phi|}$，即$|G|=|\overline{G}|\,|\ker\phi|$，所以$\overline{G}$是有限群，且$|\overline{G}|\,\big|\,|G|$.

6. 设$B_4=\{e,a,b,ab\}$是Klein四元群．$N=\{e,a\}$. 求出B_4到B_4/N的自然同态.

解 因N在B_4里的指数$[B_4:N]=2$，故由第八章，二，3，$N\lhd B_4$，从而B_4/N是商群，

且 $B_4/N=\{N,Nb\}=\{\{e,a\},\{b,ab\}\}$. 所以自然同态为

$$\begin{aligned}\phi:\ e &\to Ne &&=\{e,a\}\\ a &\to Na &&=\{e,a\}\\ b &\to Nb &&=\{b,ab\}\\ ab &\to Nab &&=\{b,ab\}\end{aligned}$$

使 $B_4\sim B_4/N$,其中 $N=\{e,a\}=\ker\phi$.

7. 设$\mathbb{C}$是全体复数对加法作成的群,$\mathbb{R}$是全体实数对加法作成的群．$\phi:a+bi\to a$ 是$\mathbb{C}$到$\mathbb{R}$的一个同态满射,使$\mathbb{C}\overset{\phi}{\sim}\mathbb{R}$.

1)　求出 $\ker\phi$.

2)　求出与$\mathbb{R}$同构的商群$\mathbb{C}/\ker\phi$.

解　1)　$\ker\phi=\{bi\mid b\in\mathbb{R}\}$. 事实上,$\forall x\in\ker\phi,x\in\mathbb{C}$,可设 $x=a+bi$,$\phi(x)=0$,又由ϕ的定义,$\phi(a+bi)=a$,从而 $a=0$,于是 $x=a+bi=bi\in\{bi\mid b\in\mathbb{R}\}$. 反之,$\forall bi\in\{bi\mid b\in\mathbb{R}\}$,由$\phi$的定义,$\phi(bi)=0$,于是 $bi\in\ker\phi$. 所以 $\ker\phi=\{bi\mid b\in\mathbb{R}\}$.

2)　由同态基本定理,$\mathbb{C}/\ker\phi\cong\mathbb{R}$. $\forall(a+bi)+\ker\phi\in\mathbb{C}/\ker\phi$,$(a+bi)+\ker\phi=(a+\ker\phi)+(bi+\ker\phi)\xlongequal{\text{由}bi\in\ker\phi}(a+\ker\phi)+\ker\phi=a+\ker\phi$. 即$\mathbb{C}/\ker\phi$中的每一个元($\ker\phi$的陪集)恰由实部相等的一切复数所组成．所以$\mathbb{C}/\ker\phi=\{a+\ker\phi\mid a\in\mathbb{R}\}$.

注　1)　因为复数可以看成是坐标平面上的点,所以 $\ker\phi$可以看做是纵轴上的一切点,而$\mathbb{C}/\ker\phi$的元就是坐标平面上的一切平行于纵轴的直线.

2)　若将ϕ改成 $\psi:a+bi\to bi$,此时,同理可得 $\ker\psi=\{a\mid a\in\mathbb{R}\}=\mathbb{R}$. $\mathbb{C}/\ker\psi=\mathbb{C}/\mathbb{R}=\{bi+\ker\psi\mid b\in\mathbb{R}\}\cong\mathbb{R}$. 即$\mathbb{C}/\ker\psi$中的每一个元($\ker\psi$的陪集)恰由虚部系数相等的一切复数所组成．于是 $\ker\psi$ 可以看做是横轴上的一切点,而$\mathbb{C}/\ker\psi$的元就是坐标平面上的一切平行于横轴的直线.

8. 首先给出定义．设ϕ是集 A 到集 $\overline{A}$ 的一个映射．若 $S\subset A$,称集$\{\phi(a)\mid a\in S\}$为 S 在ϕ下的象,记为$\phi(S)=\{\phi(a)\mid a\in S\}$. 若 $\overline{S}\subset\overline{A}$,称集$\{a\mid\phi(a)=\bar{a},\bar{a}\in\overline{S}\}$为 $\overline{S}$ 在ϕ下的逆象,记为$\phi^{-1}(\overline{S})=\{a\mid\phi(a)=\bar{a},\bar{a}\in\overline{S}\}$.

今设ϕ是群 G 到 $\overline{G}$ 的同态映射.

1)　若 $H<G$,证明:$\phi(H)<\overline{G}$.

2)　若 $\overline{H}<\overline{G}$,证明:$\phi^{-1}(\overline{H})<G$.

证　1)　因 $H<G$,故$\phi(H)$不空,且$\phi(H)\subset\overline{G}$. $\forall\bar{a},\bar{b}\in\phi(H)$,由$\phi(H)$定义,$\exists a,b\in H$,使得$\phi(a)=\bar{a}$,$\phi(b)=\bar{b}$. 于是 $\bar{a}\,\bar{b}^{-1}=\phi(a)(\phi(b))^{-1}=\phi(a)\phi(b^{-1})=\phi(ab^{-1})$. 因 $H<G$,故 $ab^{-1}\in H$. 由$\phi(H)$是 H 在ϕ下的象,$\bar{a}\,\bar{b}^{-1}\in\phi(H)$,从而$\phi(H)<\overline{G}$.

2)　因 $\overline{H}<\overline{G}$,故$\exists$单位元 $\bar{e}\in\overline{H}$. 又$\exists$单位元 $e\in G$,使$\phi(e)=\bar{e}$,从而 $e\in\phi^{-1}(\overline{H})$,即$\phi^{-1}(\overline{H})$不空．显然$\phi^{-1}(\overline{H})\subset G$. $\forall a,b\in\phi^{-1}(\overline{H})$,由$\phi^{-1}(\overline{H})$的定义,$\exists\bar{a},\bar{b}\in\overline{H}$,使$\phi(a)=\bar{a}$,$\phi(b)=\bar{b}$. 因$\phi$是同态映射,故$\phi(ab^{-1})=\phi(a)\phi(b^{-1})=\phi(a)[\phi(b)]^{-1}$. 因 $\overline{H}<\overline{G}$,故

$\phi(a)[\phi(b)]^{-1}\in\overline{H}$，即$\phi(ab^{-1})\in\overline{H}$，从而 $ab^{-1}\in\phi^{-1}(\overline{H})$. 所以$\phi^{-1}(\overline{H})<G$.

9. 用同态基本定理证明循环群 $G=(a)$的结构定理：

1） 若$|a|=\infty$，则整数加群 $\mathbb{Z}\cong G$.

2） 若$|a|=n$，则模 n 的剩余类加群 $\mathbb{Z}_n\cong G$[①].

证 显然$\phi:m\to a^m$ 是 $\mathbb{Z}$ 到 G 的一个同态满射，即 $\mathbb{Z}\overset{\phi}{\sim}G$. 由同态基本定理，$\mathbb{Z}/\ker\phi\cong G$，其中 $\ker\phi=\{k\in\mathbb{Z}\mid a^k=e\}$.

1） 若$|a|=\infty$，则 $\ker\phi=\{0\}$. 事实上，$\forall k\in\ker\phi$，有 $a^k=e$，因$|a|=\infty$，故 $k=0\in\{0\}$；反之，$\phi(0)=a^0=e$，从而 $0\in\ker\phi$. 所以 $\ker\phi=\{0\}$. 此时，$\mathbb{Z}/\ker\phi=\mathbb{Z}/\{0\}=\{m+\{0\}\mid m\in\mathbb{Z}\}=\{\{m\}\mid m\in\mathbb{Z}\}\cong\mathbb{Z}$，所以 $\mathbb{Z}\cong G$.

2） 若$|a|=n$，则 $\ker\phi=\{nq\mid q\in\mathbb{Z}\}=(n)$. 事实上，$\forall k\in\ker\phi$，$a^k=e$，于是$|a|\,\big|\,k$，即 $n\,|\,k$，从而 $\exists q\in\mathbb{Z}$，使得 $k=nq\in\{nq\mid q\in\mathbb{Z}\}$；反之，$\forall nq\in\{nq\mid q\in\mathbb{Z}\}$，$\phi(nq)=a^{nq}=(a^n)^q\xlongequal{|a|=n}e$，从而 $nq\in\ker\phi$. 所以 $\ker\phi=\{nq\mid q\in\mathbb{Z}\}$. 此时，$\mathbb{Z}/\ker\phi=\mathbb{Z}/(n)=\mathbb{Z}_n$，所以 $\mathbb{Z}_n\cong G$.

10. 命题"设 G 是交换群，则 G 的每一个子群都是不变子群"是成立的．举例说明，此命题的逆命题不成立．即：设群 G 的每一个子群都是不变子群，但 G 未必是交换群.

解 例，设$G=\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\pm\begin{pmatrix}i&0\\0&-i\end{pmatrix},\pm\begin{pmatrix}0&1\\-1&0\end{pmatrix},\pm\begin{pmatrix}0&i\\i&0\end{pmatrix}\right\}$，其中 $i^2=-1$. 由第七章，二，3，注 2)，G 对于矩阵乘法作成一个非交换群．实际上，$G=\left(\left\{\begin{pmatrix}0&1\\-1&0\end{pmatrix},\begin{pmatrix}0&i\\i&0\end{pmatrix}\right\}\right)$. 下面证明 G 的每一个子群都是不变子群．这类非交换群叫做汉弥尔顿(Hamilton)群.

我们知道，G 的子群的阶是 8 的因子，从而 G 只可能有 1，2，4，8 阶子群．1 阶、8 阶子群必是 G 的不变子群，而 4 阶子群对 G 的指数是 2. 由第八章，二，3，4 阶子群也是 G 的不变子群．最后看 2 阶子群，它是循环群，由 2 阶元生成，而 G 中 2 阶元只有一个：$\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$，于是 G 只有一个 2 阶子群 $H=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\right\}$. 由于 H 中的元都是纯量矩阵，它们与 G 中的元都可交换，即 H 是 G 的中心，从而 $H\lhd G$. 所以非交换群 G 的每一个子群都是不变子群.

11. 举例说明，Lagrange 定理的逆命题："设 G 是有限群且 $m\,\big|\,|G|$，则 G 有 m 阶子群"不成立，从而命题："设 G 是有限群且 $m\,\big|\,|G|$，则 G 有 m 阶元"也不成立.

解 例，设 $A_4=\{(1),(1\ 2\ 3),(1\ 3\ 2),(1\ 3\ 4),(1\ 4\ 3),(1\ 2\ 4),(1\ 4\ 2),(2\ 3\ 4),(2\ 4\ 3),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$. 由 A_4 对于 S_4 的乘法封闭知 $A_4<S_4$. 称 A_4 为 4 次交错群．$|A_4|=12$，又 $6\,|\,12$，但 A_4 没有 6 阶子群．事实上，若 A_4 有 6 阶子群 H，则单位元 $e=(1)\in H$. 因 A_4 中有且只有 3 个 2 阶元$(ab)(cd)(a,b,c,d\in\{1,2,3,4\})$，故 6 阶

① 张禾瑞．近世代数基础．北京：高等教育出版社，1978. 59. 定理．

子群 H 中必有 3－循环置换$(abc)\big(a,b,c\in\{1,2,3,4\}\big)$，于是$(abc)$的逆元$(abc)^{-1}=(acb)\in H$. 因而在 H 中，3－循环置换成对出现．又$(1)\in H$，于是 H 中至少含一个 2 阶元，不妨设为$(ab)(cd)$. 因此，$(abc)[(ab)(cd)]=(bdc)\in H$，$[(ab)(cd)](abc)=(acd)\in H$，$(acd)^{-1}=(adc)\in H$，即 H 中至少有 7 个元：(1)，$(abc)(acb)$，$(ab)(cd)$，(bdc)，(acd)，(adc). 此与 $|H|=6$ 矛盾．所以 A_4 中没有 6 阶子群.

12. 设 $H<G$，证明：$H\lhd G$ 的充分与必要条件是 H 的任意两个左陪集的乘积仍是一个左陪集(即 H 的所有左陪集的集合 S 对于乘法封闭).

证一　(⇒)　$\forall x,y\in G$，$\forall h,h_1\in H$，$(xh)(yh_1)=x(hy)h_1$. 因 $H\lhd G$，故 $hy\in Hy=yH$，从而 $\exists h_2\in H$，使得 $hy=yh_2$，于是$(xh)(yh_1)=x(yh_2)h_1=(xy)(h_2h_1)\in(xy)H$. 由 h,h_1 是 H 中任意元，有$(xH)(yH)\subset(xy)H$. 反之，$\forall h'\in H$，$(xy)h'=(xe)(yh')\in(xH)(yH)$，因此$(xy)H\subset(xH)(yH)$. 所以$(xH)(yH)=(xy)H$. 至于这个乘法是 S 的一个代数运算的证明留给读者.

(⇐)　已知 $H<G$ 且 $\forall x,y\in G$，$(xH)(yH)$仍是一个左陪集，从而 $\exists z\in G$，使得$(xH)(yH)=zH$. 于是 $xy=(xe)(ye)\in(xH)(yH)=zH$. 因此 $zH=(xy)H$，即$(xH)(yH)=(xy)H$. $\forall x\in G,h\in H$，$xhx^{-1}=(xh)(x^{-1}e)\in(xH)(x^{-1}H)=(xx^{-1})H=eH=H$. 所以 $H\lhd G$.

证二　(⇒)　见证一.

(⇐)　由已知，$\forall x\in G$，可设$(xH)(x^{-1}H)=zH$. 因 $e=(xe)(x^{-1}e)\in(xH)(x^{-1}H)=zH$，故 $zH=eH=H$. 即$(xH)(x^{-1}H)=H$. $\forall x\in G,h\in H$，$xhx^{-1}=(xh)(x^{-1}e)\in(xH)(x^{-1}H)=H$. 所以 $H\lhd G$.

注　1)　由该命题知下面结论：设 $H<G$，则 $H\lhd G$ 的充分与必要条件是 H 的所有左陪集的集合 S 对于乘法来说作成一个群.

2)　举一例说明，当子群 H 不是 G 的不变子群时，H 的所有左陪集的集合 S 对于乘法来说不能作成一个群．设 $H=\{(1),(1\ 2)\}<S_3$，H 不是 S_3 的不变子群．$S=\{H,(1\ 3)H,(2\ 3)H\}$. $(13)H=(1\ 3\ 2)H$，$(2\ 3)H=(1\ 2\ 3)H$，而$\big((1\ 3)H\big)\big((2\ 3)H\big)=\big((1\ 3)(2\ 3)\big)H=(123)H$，$\big((132)H\big)\big((123)H\big)=\big((132)(123)\big)H=(1)H$，因此$\big((13)H\big)\big((23)H\big)\neq\big((1\ 3\ 2)H\big)\big((1\ 2\ 3)H\big)$. 从而$(xH)(yH)=(xy)H$ 不是 S 的一个代数运算．所以 S 不能作成一个群.

13. 设ϕ是群 G 到群 $\overline{G}$ 的一个同态映射，e 是 G 的单位元，$\bar{e}$ 是 $\overline{G}$ 的单位元．$\ker\phi=\{a\in G\mid\phi(a)=\bar{e}\}$. 证明：

$$\phi\text{是单射}\Leftrightarrow\ker\phi=\{e\}.$$

证　(⇒)　$\forall x\in\ker\phi$，$\phi(x)=\bar{e}$，又$\phi(e)=\bar{e}$，从而$\phi(x)=\phi(e)$. 因ϕ是单射，故 $x=e$. 所以 $\ker\phi=\{e\}$.

(⇐)　$\forall a,b\in G$，若$\phi(a)=\phi(b)$，下面证 $a=b$. $\phi(a)(\phi(b))^{-1}=\bar{e}$，即$\phi(ab^{-1})=\bar{e}$，从而 $ab^{-1}\in\ker\phi$．因 $\ker\phi=\{e\}$，故 $ab^{-1}=e$，于是 $a=b$. 所以ϕ是单射.

14. 设 $N\lhd G$，证明：

1)　$\overline{H}<G/N\Leftrightarrow\overline{H}=H/N,N\subset H<G$.

2） 若 $N\subset H<G$，那么 $H\lhd G \Leftrightarrow H/N\lhd G/N$.

证一 1） （⇒） $\phi: a\to aN$ 是 G 到 G/N 的自然同态，使 $G\overset{\phi}{\sim}G/N$ 且 $N=\ker\phi$. 因 $\overline{H}<G/N$，故 $H=\phi^{-1}(\overline{H})<G$. $H\supset\ker\phi=N$. 事实上，$\forall a\in\ker\phi=N$，$\phi(a)=aN=N$. 又 $\overline{H}<G/N$，从而 G/N 的单位元 $N\in\overline{H}$，于是 N 在 ϕ 下的逆象 $a\in\phi^{-1}(\overline{H})=H$，所以 $N\subset H$. 由第八章，二，7，因 H 是 $\overline{H}$ 的逆象，故 $\overline{H}$ 是 H 的象，即 $\overline{H}=\phi(H)$. 因 $N\lhd G$，$N\subset H<G$，故由第八章，三，2，5），$N\lhd H$，从而 $\phi(H)=\{hN\,|\,h\in H\}=H/N$. 所以 $\overline{H}=H/N$.

（⇐） 已知 $N\lhd G$，$N\subset H<G$，于是 $N\lhd H$，从而 $\overline{H}=H/N$ 是群．$\forall hN\in H/N$，有 $hN\in G/N$，从而 $H/N\subset G/N$. 又 H/N 对于 G/N 的乘法作成群，所以 $\overline{H}=H/N<G/N$.

2） 因 $N\lhd G$，$N\subset H<G$，故 $N\lhd H$. 又 $G\overset{\phi}{\sim}G/N$，其中 ϕ 是自然同态：$a\to aN$，$N=\ker\phi$. 于是 $\phi(H)=\{hN\,|\,h\in H\}=H/N$.

（⇒） 因 $H\lhd G$，故 $\phi(H)=H/N\lhd G/N$[①].

（⇐） 由第八章，二，7，注 3），$\phi^{-1}(H/N)\xlongequal{\text{由 } N=\ker\phi}HN\xlongequal{\text{由 } N\subset H}H$. 因 $H/N\lhd G/N$，故 $\phi^{-1}(H/N)=H\lhd G$.

证二 1） 见证一.

2） （⇒） $\forall gN\in G/N, g\in G$，$\forall hN\in H/N, h\in H$，$(gN)(hN)(gN)^{-1}=(ghg^{-1})N$. 因 $H\lhd G$，故 $ghg^{-1}\in H$，从而 $(gN)(hN)(gN)^{-1}\in H/N$. 再由1），$H/N<G/N$. 所以 $H/N\lhd G/N$.

（⇐） 已知 $H<G$. $\forall g\in G, h\in H$，因 $H/N\lhd G/N$，故 $(gN)(hN)(gN)^{-1}=(ghg^{-1})N\in H/N$. 从而 $\exists h'\in H$，使得 $(ghg^{-1})N=h'N$. 于是 $\exists n\in N$，使得 $ghg^{-1}=h'n$. 又 $N\subset H<G$，因此 $ghg^{-1}\in H$. 所以 $H\lhd G$.

15. 证明：1） 设 $a\in$ 群 G，$Z(a)=\{x\in G\,|\,xa=ax\}$，则 $Z(a)<G$. 称 $Z(a)$ 是元 a 在 G 内的中心化子，或称 $Z(a)$ 是元 a 在 G 内的正规化子.

2） 设 $S\subset$ 群 G，$S\neq\varnothing$，$Z(S)=\{x\in G\,|\,\forall s\in S, xs=sx\}$，则 $Z(S)<G$. 称 $Z(S)$ 是集 S 在 G 内的中心化子.

3） 设 $S\subset$ 群 G，$S\neq\varnothing$，$N(S)=\{x\in G\,|\,xS=Sx\}$，则 $N(S)<G$. 称 $N(S)$ 是集 S 在 G 内的正规化子.

4） 设 $H<G$，则 $H\lhd G\Leftrightarrow N(H)=G$.

5） 设 $H<G$，则 $H\lhd N(H)$.

6） 设 $H<G$，则 $Z(H)\lhd N(H)$.

7） 设 $H\lhd G$，则 $Z(H)\lhd G$.

证 1） 显然 $Z(a)\subset G$. 因 $aa=aa$，故 $a\in Z(a)$，从而 $Z(a)\neq\varnothing$. $\forall x,y\in Z(a)$，$xa=ax$，$ya=ay$，于是 $ay^{-1}=y^{-1}a$. 因此 $(xy^{-1})a=x(y^{-1}a)=x(ay^{-1})=(xa)y^{-1}=(ax)y^{-1}=a(xy^{-1})$. 可见 $xy^{-1}\in Z(a)$. 所以 $Z(a)<G$.

---

① 张禾瑞．近世代数基础．北京：高等教育出版社，1978. 77. 定理 3.

2) $\forall s\in S$，因 $es=se$，故 $e\in Z(S)\neq\varnothing$. 显然 $Z(S)\subset G$. $\forall x,y\in Z(S)$，$\forall s\in S$，$xs=sx$，$ys=sy$. 于是 $(xy)s=x(ys)=x(sy)=(xs)y=(sx)y=s(xy)$，从而 $xy\in Z(S)$. $\forall x\in Z(S)$，$\forall s\in S$，$xs=sx$ 两端左、右各乘 x^{-1}，得 $sx^{-1}=x^{-1}s$，从而 $x^{-1}\in Z(S)$. 所以 $Z(S)<G$.

3) 因 $eS=Se$，故 $e\in N(S)\neq\varnothing$. 显然 $N(S)\subset G$. $\forall x,y\in N(S)$，$xS=Sx$，$yS=Sy$. 于是 $(xy^{-1})S=(xy^{-1})S(yy^{-1})=xy^{-1}(Sy)y^{-1}=xy^{-1}(yS)y^{-1}=x(y^{-1}y)Sy^{-1}=(xS)y^{-1}=(Sx)y^{-1}=S(xy^{-1})$，从而 $xy^{-1}\in N(S)$. 所以 $N(S)<G$.

4) $H\lhd G\Leftrightarrow\forall g\in G,gH=Hg\Leftrightarrow\forall g\in G,g\in N(H)\Leftrightarrow G=N(H)$.

5) $\forall h\in H$，因 $H<G$，故 $hH=H=Hh$，从而 $h\in N(H)$，于是 $H\subset N(H)$. 又 H 对于 $N(H)$ 的代数运算作成一个群，所以 $H<N(H)$. $\forall x\in N(H)$，有 $xH=Hx$，从而 $H\lhd N(H)$.

6) $\forall z\in Z(H)$，$\forall h\in H$，有 $zh=hz$，从而 $zH=Hz$，于是 $z\in N(H)$，因此 $Z(H)\subset N(H)$. 又 $Z(H)$ 对于 $N(H)$ 的代数运算作成一个群，所以 $Z(H)<N(H)$. $\forall g\in N(H)$，$\forall z\in Z(H)$，要证 $Z(H)\lhd N(H)$，只需证 $gzg^{-1}\in Z(H)$，只需证 $\forall h\in H,gzg^{-1}h=hgzg^{-1}$. 我们来看：$\forall h\in H,gzg^{-1}h(gzg^{-1})^{-1}=gz(g^{-1}hg)z^{-1}g^{-1}$. 因 $g\in N(H)$，故 $Hg=gH$，从而 $hg\in Hg=gH$，于是 $\exists h'\in H$，使得 $g^{-1}hg=g^{-1}gh'=h'\in H$. 又 $z\in Z(H)$，故 z 与 $g^{-1}hg$ 可交换，因此 $gzg^{-1}h(gzg^{-1})^{-1}=gg^{-1}hgzz^{-1}g^{-1}=h$，即 $\forall h\in H,gzg^{-1}h=hgzg^{-1}$，从而 $gzg^{-1}\in Z(H)$. 所以 $Z(H)\lhd N(H)$.

7) 由 6)，有 $Z(H)\lhd N(H)$. 今 $H\lhd G$，由 4)，$N(H)=G$，从而 $Z(H)\lhd G$.

注 1) $Z(e)=G$.

2) 设 G 是交换群，则 $\forall a\in G,Z(a)=G$.

3) G 的中心是 G 在 G 内的中心化子 $Z(G)$.

4) 若 $|G|\geqslant 2$，则 $|Z(a)|\geqslant 2$. 因为当 $a=e$ 时，$Z(a)=G$，从而 $|Z(a)|=|G|\geqslant 2$；当 $a\neq e$ 时，$a\in Z(a)$ 且 $e\in Z(a)$，从而 $|Z(a)|\geqslant 2$.

四、思考问题

1. 试判断下面群 G 的子群 H 是否为 G 的不变子群.

1) $G=\{e,a,b,c,d,f\}$，其中

$$e=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix},a=\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix},b=\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix},$$

$$c=\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix},d=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix},f=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}.$$

G 对于矩阵乘法作成一个群. $H=\{e,a\}<G$.

2) $G=\left\{\mathbb{R}\text{ 的变换 }\tau_{ab}\,\middle|\,\tau_{ab}:x\rightarrow ax+b,a,b\in\mathbb{Q},a\neq 0\right\}$ 对于变换乘法作成一个群. $H=\left\{\mathbb{R}\text{ 的变换 }\tau_{1b}\,\middle|\,\tau_{1b}:x\rightarrow x+b,b\in\mathbb{Q}\right\}<G$（见第七章，四，1，7））.

2. 设 $N \lhd G$，试写出商群 G/N.

1) G 是模 9 的剩余类加群，$N=([3])\lhd G$.

2) $G=(a)$ 是 15 阶循环群，$N=(a^3)\lhd G$.

3) G 是有理数集对于加法作成的群，N 是整数加群，$N\lhd G$.

3. 设 $N\lhd G$. 试写出下面各商群 G/N 的元，并证明：$G/N\cong \overline{G}$.

1) $N=\{(1),(12)(34),(13)(24),(14)(23)\}$，$G=S_4$，$N\lhd G$（见第八章，二，5）. $\overline{G}=S_3$.

2) $N=\left\{\begin{pmatrix}1 & c\\ 0 & 1\end{pmatrix}\middle| c\in\mathbb{Q}\right\}$，$G=\left\{\begin{pmatrix}a & b\\ 0 & 1\end{pmatrix}\middle| a,b\in\mathbb{Q},a\neq 0\right\}$，$N\lhd G$，（见第八章，二，5）. $\overline{G}$ 是全体有理数集对于乘法作成的群.

4. 设 $H_i<G$，$i=1,2,3,4$. 试判断下面命题是否正确.

1) 若 $H_1H_3=H_2H_3$，则 $H_1=H_2$.

2) 若 $H_1\subset H_2$，$H_3\subset H_4$，则

$$(H_1H_3)\cap H_2\cap H_4=(H_1\cap H_4)(H_2\cap H_3).$$

3) 若 $H_i\lhd G$，$i=1,2,3$，且 $H_1\subset H_2$，则 $H_1H_3\lhd H_2H_3$.

5. 设 H 与 K 都是群 G 的有限子群，证明：乘积 HK 中含元的个数 $|HK|=\dfrac{|H|\cdot|K|}{|H\cap K|}$.

6. 证明：6 阶群 G 至多含有一个 3 阶子群.

7. 设 $H_1,H_2,\cdots,H_n$ 都是群 G 的有限不变子群，$|H_1|,|H_2|,\cdots,|H_n|$ 两两互素．证明：$|H_1H_2\cdots H_n|=|H_1|\cdot|H_2|\cdots|H_n|$.

8. 设群 G 的子群 H 是循环群．证明：H 的共轭子群 S 仍是循环群.

9. 找出包含不空子集 S 的群 G 的最小不变子群.

10. 令 π 和 $(i_1i_2\cdots i_k)$ 属于 S_n. 证明：

$$\pi^{-1}(i_1i_2\cdots i_k)\pi=(i_1^{\pi}i_2^{\pi}\cdots i_k^{\pi}),$$

即在 S_n 里，$(i_1i_2\cdots i_k)$ 的共轭置换 $\pi^{-1}(i_1i_2\cdots i_k)\pi$ 就是将 $(i_1i_2\cdots i_k)$ 中的每个数字 i_t 换成 i_t^{π} 所得的置换，$t=1,2,\cdots,k$.

11. 当 $n\geqslant 3$ 时，证明：S_n 的中心 $Z=\{(1)\}$.

12. 设 G 为非交换群，Z 是 G 的中心，证明：G/Z 不是循环群.

13. 证明：$GL_2(\mathbb{R})$ 的中心 Z 由所有 $\mathbb{R}$ 上的 2 阶可逆纯量矩阵组成，即 $Z=\left\{\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}\middle| a\in\mathbb{R},a\neq 0\right\}$.

14. 设 $\mathbb{R}^*$ 是全体非零实数集．卡氏积 $\mathbb{R}^*\times\mathbb{R}$ 对于代数运算：$(a,b)(c,d)=(ac,bc+d)$ 作成一个群. 求元 $(1,1)$ 在 $\mathbb{R}^*\times\mathbb{R}$ 内的中心化子 $Z\big((1,1)\big)$.

15. 设 G 是交换群，$H<G$，$a\in G$，$a,a^2,\cdots,a^{n-1}\overline{\in} H$，但 $a^n\in H$. 假定 a 是有限阶元．求证：n 是 a 的阶 $|a|$ 的因子，且 n 等于商群 G/H 中元 aH 的阶 $|aH|$.

16. 设 G 是交换群，H 是 G 中一切有限阶元所成的集．证明：$H\lhd G$，且 G/H 中除单位元外，不含有限阶的元.

17. 证明：$N\lhd G\Leftrightarrow \forall a\in G,\exists b\in G$，使得 $aN=Nb$.

18. 设 $N_1 \lhd G, N_2 \lhd G$ 且 $N_1 \cap N_2 = \{e\}$，证明：$\forall x \in N_1, y \in N_2$，都有 $xy = yx$.

19. 设 $A < G, B < G, C < G$ 且 $A \lhd B$. 证明：$C \cap A \lhd C \cap B$.

20. 设 $H \lhd G, K \lhd G$，且 $G/H, G/K$ 是交换群. 证明：$G/H \cap K$ 也是交换群.

21. 若群 $G(\neq \{e\})$ 除 $\{e\}$ 及 G 以外无其他不变子群，则称 G 为单群. 设 G 是有限交换群. 证明：G 是单群的充分必要条件是 G 的阶 $|G|$ 是素数.

22. 若群 $G(\neq \{e\})$ 除 $\{e\}$ 及 G 以外无其他不变子群，则称 G 为单群. 设 G 是单群，且 $G \sim \overline{G}$. 证明：$\overline{G}$ 是单群或 $\overline{G} = \{\bar{e}\}$，其中 $\bar{e}$ 是 $\overline{G}$ 的单位元.

23. 设 G 是有限群，$N \lhd G$，且 $(|N|, [G:N]) = 1$，证明：阶为 $|N|$ 的因数的 G 的子群 H 必为 N 的子群.

24. 设 $K \lhd H, H \lhd G, |K| = n, |H| = nm, (n, m) = 1$，证明：$K \lhd G$.

25. 设 $\forall g \in$ 群 G，$\forall$ 自然数 n，方程 $x^n = g$ 在 G 内恒有解，证明：$\forall H \lhd G, H \neq G$，$[G:H] = \infty$.

26. 证明：1）　设 F 是数域，F 对于普通加法来说作成一个交换群. 则 $\forall H < F, H \neq F$，有 $[F:H] = \infty$.

2）　数域 F 上全体 n 阶矩阵集 M 对于矩阵加法来说作成一个交换群. 则 $\forall H < M$，$H \neq M$，有 $[M:H] = \infty$.

3）　数域 F 上全体一元多项式集 $F(x)$ 对于多项式加法来说作成一个交换群. 则 $\forall H < F[x], H \neq F[x]$，有 $[F[x]:H] = \infty$.

27. 设 G 是群，将换位子 $a^{-1}b^{-1}ab$ 记为 $[a,b]$. $\forall a, b, c \in G$，证明：

1）　$[a,b]^{-1} = [b,a]$.

2）　$[ab,c] = b^{-1}[a,c]b[b,c]$
$= [a,c][[a,c],b][b,c]$.

3）　$[a,bc] = [a,c]c^{-1}[a,b]c$
$= [a,c][a,b][[a,b],c]$.

4）　$[a^{-1},b^{-1}] = ab[a,b](ab)^{-1}$.

5）　$[a,b^{-1}] = b[b,a]b^{-1}$.

6）　$[a^{-1},b] = a[b,a]a^{-1}$.

下面假定任一换位子 $[a,b]$ 与 G 中任一元 g 可交换，即 $[a,b]g = g[a,b]$. 证明：

7）　$[ab,c] = [a,c][b,c]$.

8）　$[a,bc] = [a,b][a,c]$.

9）　$[a^{-1},b^{-1}] = [a,b]$.

10）　$[[a,b],c] = [a,[b,c]]$.

11）　$[a,b]^{-1}c = c[a,b]^{-1}$.

28. 设 $N \lhd G$，N 具有有限指数 n，$t \in G$，且 h 是使 $t^h \in N$ 的最小正整数. 证明：$h \mid n$. 如果 t 的阶有限，$|t| = r$，证明：$h \mid r$.

29. 设 $x \in$ 群 G，元 x 在 G 内的中心化子 $Z(x) = \{a \in G \mid xa = ax\} < G$（见第八章，三，15，1)). 设 $D = \{y \in G \mid y = gxg^{-1}, g \in G\}$，即 D 含与 x 共轭的所有的元（见第八章，一，7，

1)). 若 G 是有限群,证明:D 含元的个数$=[G:Z(x)]$.

30. 设 Z 是阶为 p^n(p 是素数)的群 G 的中心,证明:Z 中至少含两个元.

31. 设 G 是 p^2 阶群,p 是素数,证明:G 是交换群.

32. 设 $H \lhd G$, $|G|=p^n$, p 是素数, $|H|=p$, Z 是 G 的中心,证明:$H \subset Z$.

33. 设 G 是有限交换群,$|G|=n$, p 是素数, $p \mid n$. 证明:G 中存在阶为 p 的元. 从而 G 有 p 阶循环子群.

34. 设 p,q 是互异素数,$|G|=pq$. 证明:G 中存在 q 阶子群.

35. 若素数 $p \mid |G|$,证明:群 G 有 p 阶元. 从而 G 有 p 阶循环子群.

36. 设 p,q 是互异素数,$|G|=pq$, G 是交换群. 证明:G 是循环群.

37. 设 $p<q$, q 是素数. 证明:pq 阶群 G 不能有两个不同的 q 阶子群.

38. 设 p,q 都是素数,$p<q$. 证明:pq 阶群 G 的 q 阶子群必为不变子群.

39. 设 G 是有限群,$p \mid |G|$, p 是素数,若方程 $x^p=e$ 在 G 内恰有 p 个解,证明:这 p 个解的集 $H=\{x \in G \mid x^p=e\}$ 是 G 的不变子群.

40. 判断下面各命题是否正确.

1) ϕ是群 G 到 G 的同态映射

$\Leftrightarrow \phi$是群 G 到 G 的一个子群 G_1 的同态满射.

2) 设 A 与 B 都是群,若存在 B'是 B 的真子群,使 $A \cong B'$;存在 A'是 A 的真子群,使 $B \cong A'$,则 A 与 B 都分别与自己的一个真子群同构.

3) 设群 $G \overset{\phi}{\sim}$ 群 $\overline{G}$,且 H_1, H_2 是 G 的不同子群,则$\phi(H_1)$, $\phi(H_2)$是 $\overline{G}$ 的不同子群.

4) 设群 $G \overset{\phi}{\sim}$ 群 $\overline{G}$, A,B 都是 G 的子群,$A \supset B$,且 A,B 在ϕ下的象分别是 $\overline{A}, \overline{B}$,则$\overline{A} \supset \overline{B}$.

5) 设群 $G \overset{\phi}{\sim}$ 群 H,群 $G \overset{\psi}{\sim}$ 群 K,若 $\ker \phi = \ker \psi$,则 $H \cong K$.

6) 设 $G=(g)$是循环群,$|G|=n=st$. $H_1=(g^s)$与 $H_2=(g^t)$是 G 的子群,则 $H_1 \lhd G$, $H_2 \lhd G$,且 $G/H_1 \cong H_2$, $G/H_2 \cong H_1$.

41. 设下面各ϕ是群 G 到群 $\overline{G}$ 的同态满射,试写出ϕ的核 $\ker \phi$.

1) G 是整数加群,$\overline{G}=\{1,-1\}$对于普通乘法作成一个群. $\phi: n \to \begin{cases} 1, n \text{ 是偶数时}; \\ -1, n \text{ 是奇数时}. \end{cases}$

2) G 是全体非零实数集对于普通乘法作成的群,$\overline{G}=G$. $\phi: x \to \dfrac{1}{x}$.

3) G 是全体非零实数集对于普通乘法作成的群,$\overline{G}$ 是全体正实数集对于普通乘法作成的群. $\phi: x \to |x|$.

4) $G=\{1,-1,\mathrm{i},-\mathrm{i}\}$, $\overline{G}=\{1,-1\}$. $\phi: 1 \to 1, -1 \to 1, \mathrm{i} \to -1, -\mathrm{i} \to -1$.

5) G 是整数加群,$\overline{G}=\{1,-1,\mathrm{i},-\mathrm{i}\}$. $\phi: n \to \mathrm{i}^n$.

6) G 是整数加群,$\overline{G}=\{[0],[1],[2],\cdots,[n-1]\}$ 是模 n 的剩余类加群. $\phi: a \to [a]$.

7) $G=\{[0],[1],[2],\cdots,[7]\}$是模 8 的剩余类加群. $\overline{G}=\{[0],[1]\}$是模 2 的剩余类加群. $\phi: [n] \to \begin{cases} [0], n \text{ 是偶数时}; \\ [1], n \text{ 是奇数时}. \end{cases}$

8)　$G=(a)=\{a^0=e,a,a^2,\cdots,a^5\}$是 6 阶循环群，$\overline{G}=\{e,a^3\}=(a^3)$是 2 阶循环群．$\phi:e\to e.\ a\to a^3,a^2\to e,a^3\to a^3,a^4\to e,a^5\to a^3$.

9)　$G=\{[0],[1],[2],\cdots,[11]\}$是模 12 的剩余类加群，$\overline{G}=\{1,-1,\mathrm{i},-\mathrm{i}\}$. $\phi:[n]\to \mathrm{i}^n$.

10)　G 是任意一个群，$\overline{G}$ 也是任意一个群，$\overline{e}$ 是 $\overline{G}$ 的单位元．$\phi:x\to\overline{e}$.

11)　$G=GL_n(\mathbb{R})$是实数域$\mathbb{R}$上的一切 n 阶可逆方阵集对于矩阵乘法作成的群，$\overline{G}$ 是全体非零实数集对于普通乘法作成的群．$\phi:A\to|A|$.

12)　G 是整数加群，$\overline{G}=(a)$是循环群．$\phi:n\to a^n$.

13)　G 是交换群，取定 $k\in\mathbb{Z}$，$\overline{G}=\{a^k\,|\,a\in G\}$. $\phi:a\to a^k$.

14)　G 是全体正有理数的集对于普通乘法作成的群，$\overline{G}$ 是整数加群．$\forall a\in G$，a 可唯一地表成 $a=2^n\dfrac{q}{p}$，其中 n 是整数，p,q 是奇数．$\phi:a\to n$.

15)　$G=GL_2(\mathbb{Q})$是有理数域$\mathbb{Q}$上的一切 2 阶可逆方阵集对于矩阵乘法作成的群，$\overline{G}=\left\{\begin{pmatrix}1&n\\0&1\end{pmatrix}\,\middle|\,n\in\mathbb{Z}\right\}$. $\forall A\in G$，$|A|$可唯一地表成$|A|=2^n\dfrac{q}{p}$，其中 n 是整数，$p,q\in\mathbb{Z}$，p,q 是奇数．$\phi:A\to\begin{pmatrix}1&n\\0&1\end{pmatrix}$.

16)　$G=\{\tau_{ab}\,|\,\forall x\in\mathbb{R},x^{\tau_{ab}}=ax+b,a,b\in\mathbb{R},a\neq0\}$是$\mathbb{R}$的一个变换群(见第五章，二，3)，$\overline{G}$ 是全体非零实数集对于普通乘法作成的群．$\phi:\tau_{ab}\to a$.

17)　$G=\{2^m3^n\,|\,m,n\in\mathbb{Z}\}$对于普通乘法作成一个群，$\overline{G}=\{2^m\,|\,m\in\mathbb{Z}\}$对于普通乘法也作成一个群．$\phi:2^m3^n\to 2^m$.

42. 设 G 是由集 S 生成的群，ϕ 是群 G 到群 $\overline{G}$ 的同态满射．证明：集 S 在ϕ下的象$\phi(S)$生成群$\overline{G}$.

43. 设 $H\lhd G,[G:H]=m$. 证明：$\forall g\in G$，都有 $g^m\in H$.

44. 设 G 是有理数集对于普通加法来说作成的群．证明：$\forall H<G,H\neq G$，有$[G:H]=\infty$.

45. 设 G 是非零复数集对于普通乘法来说作成的群．证明：$\forall H<G,H\neq G$，有$[G:H]=\infty$.

46. 设 $N\lhd G,H\lhd G,N\subset H$. 证明：$G/H\cong(G/N)/(H/N)$.

47. 设 $N\lhd G,H\lhd G$. 证明：$G/NH\cong(G/N)/(NH/N)$.

48. 设 $N\lhd G,H<G$. 证明：$N\cap H\lhd H$ 且 $H/(N\cap H)\cong NH/N$.

49. 设 G 是有限群．$N\lhd G$. $|N|=n,|G/N|=m,(m,n)=1$. 证明：N 是 G 的唯一的一个阶为 n 的子群.

50. 取定 $a\in$ 群 G，$\forall x\in G,\phi_a:x\to axa^{-1}$是 G 的一个内自同构(见第八章，一，7，3)). $I(G)=\{\phi_a\,|\,a\in G\}$是 G 的所有的内自同构的集．已知 G 的所有自同构的集对于变换乘法来说作成一个群，记为 $AutG$，称 $AutG$ 为群 G 的自同构群．证明：

1)　$G\sim I(G)$. 从而 $I(G)$对于变换乘法来说作成一个群，称 $I(G)$为群 G 的内自同构群，且ϕ_e 是 $I(G)$的单位元，其中 e 是 G 的单位元.

2)　若 Z 是 G 的中心，则 $G/Z\cong I(G)$.

3)　$I(G)\lhd AutG$.

第九章　加群、环的定义、整环

一、基本问题问答

1. 环的三大来源是什么？

答　整数环$\mathbb{Z}$、数域F上的一元多项式环$F[x]=\{f(x)\mid f(x)$的系数在数域F中$\}$和数域F上的$n\times m$矩阵环.

2. 环的两个代数运算：加法与乘法的关系是什么？

答　所谓两个代数运算是指一个代数运算不能用另外一个代数运算来代替，不能由一个代数运算的存在就导出另一个代数运算的存在，谁也推不出谁来. 但是，环的两个代数运算又不是孤立的，而是通过乘法对于加法的左、右分配律紧密联系在一起的. 在环中两个代数运算通过分配律溶为一体，由此才形成了具有两个代数运算的环的结构理论.

例　设$\mathbb{Z}$是整数加群. $\forall a,b\in\mathbb{Z}$，规定$ab=a$，这是$\mathbb{Z}$的一个代数运算且适合结合律. 但$3(1+1)=3\neq 6=3+3=3\cdot 1+3\cdot 1$，从而不适合左分配律. 因此$\mathbb{Z}$对于这两个代数运算来说不能作成一个环.

3. 1)　加群G的零元与元a的负元是如何定义的？又如何判别？

2)　加群G中元的差是如何定义的？又如何判别？

答　1)　加群G的单位元叫做G的零元，记为0. 即：$b\in G$，

$$b\text{是}G\text{的零元}\Leftrightarrow\forall a\in G,b+a=a.$$

实际上可如下判别：$b\in G$，

$$b=0\Leftrightarrow\exists a\in G,\text{使得 }b+a=a.$$

例　要证明$0a=0$，其中$a\in$环R，0是环R(R当然是加群)的零元. 因$0a=(0+0)a=0a+0a$，故由判别条件，$0a=0$.

加群G中元a的逆元叫做a的负元，记为$-a$. 判别方法为：$a,b\in$加群G，

b是a的负元：$b=-a\Leftrightarrow b+a=0$.

例　设R是一个有单位元1的环，$a\in R$，证明：$(-1)a=-a$.

证　因$(-1)a+a=(-1)a+1a=(-1+1)a=0a=0$，由判别条件，$(-1)a=-a$.

当然，直接利用定义也可证明：$(-1)a=1(-a)=-a$.

2)　$\forall a,b\in$加群G，定义a与b的差为$a+(-b)$，记为$a-b=a+(-b)$. 判别方法为：$a,b,c\in$加群G，

$$c=a-b\Leftrightarrow b+c=a.$$

4. 环R的可逆元的定义是什么？如何判别？

答　设R是有单位元1的环，

$$a\in R, a\text{ 是环 }R\text{ 的可逆元}\overset{\text{定义}}{\Longleftrightarrow}\exists b\in R,$$

使得 $ba=ab=1$. b 称为 a 的逆元,记为 $b=a^{-1}$.

判别条件为:$a,b\in$有单位元 1 的环 R,

$$b=a^{-1}\Leftrightarrow ba=ab=1.$$

例　设 a 是有单位元 1 的环 R 的一个可逆元,证明:$-a$ 也是可逆元,且 $(-a)^{-1}=-a^{-1}$.

证　因 a 可逆,故 $\exists a^{-1}\in R$,使得 $a^{-1}a=aa^{-1}=1$,从而 $(-a^{-1})(-a)=a^{-1}a=1$,$(-a)(-a^{-1})=aa^{-1}=1$. 由判别条件,$-a$ 是可逆元,且 $(-a)^{-1}=-a^{-1}$.

读者可用同样方法证明:若 a,b 是有单位元 1 的环 R 的两个可逆元,则 ab 也可逆,且 $(ab)^{-1}=b^{-1}a^{-1}$.

注　粗略地讲,环 R 的可逆元就是整除单位元的元.

5. 设 $a\in$环 R,n 是正整数. 若 $n\in R$,能否将 a 的 n 倍 na 看成是环 R 中两个元 n 与 a 的积呢?

答　不能. 例,设 $\mathbb{Z}$ 是整数加群,定义乘法为 $ab=0$,则 $\mathbb{Z}$ 是一个环. 取 $2\in\mathbb{Z}$,正整数 $3\in\mathbb{Z}$,于是 2 的 3 倍 $3(2)=2+2+2=6$,但 3 与 2 的积却为 0.

当环 R 有单位元 1 时,

$$na=n(1a)=\overbrace{1a+1a+\cdots+1a}^{n\text{个}}=(\overbrace{1+1+\cdots+1}^{n\text{个}})a=(n1)a,$$

从而 a 的 n 倍是 R 中两个元 $n1$ 与 a 的积.

6. 含任意有限多个元的环是否都存在?

答　存在. 设 n 是任意一个正整数,则模 n 的剩余类环 $\mathbb{Z}_n=\{[0],[1],\cdots,[n-1]\}$ 就恰含 n 个元.

注　1)　在证明 $[a]+[b]=[a+b]$ 与 $[a][b]=[ab]$ 是 $\mathbb{Z}_n$ 的两个代数运算时,需注意证明和与积的唯一性,不受代表选择的影响.

2)　$\mathbb{Z}_n$ 的零元 $0=[0]$,$[a]$ 的负元 $-[a]=[-a]$,$\mathbb{Z}_n$ 的单位元 $1=[1]$.

7. a 是环 R 的左(右)零因子与零因子的定义分别是什么? 如何判别环 R 有无零因子?

答　a 是环 R 的左(右)零因子 $\Leftrightarrow$ 1)　$a\in$环 R,$a\neq 0$;

2)　$\exists b\in R$,$b\neq 0$,使得 $ab=0$ $(ba=0)$.

a 是环 R 的零因子 $\Leftrightarrow$ a 既是环 R 的左零因子,又是环 R 的右零因子.

环 R 有零因子 $\Leftrightarrow$ $\exists a,b\in$环 R,$a\neq 0$,$b\neq 0$,使得 $ab=0$.

环 R 无零因子 $\Leftrightarrow$ 环 R 既无左零因子,又无右零因子

$\Leftrightarrow$ $\forall a,b\in$环 R,$a\neq 0$ 且 $b\neq 0$ 时,$ab\neq 0$

$\Leftrightarrow$ $\forall a,b\in$环 R,$ab=0$ 时,$a=0$ 或 $b=0$

$\Leftrightarrow$ $\forall a,b\in$环 R,若 $ab=0$,$a\neq 0$,则 $b=0$.

(常用最后一种形式来判别 R 无零因子)

注　1)　环 R 有左零因子 $\Leftrightarrow$ 环 R 有右零因子.

2)　粗略地说,环 R 的零因子就是零元 0 的非零因子,或说环 R 的零因子就是整除零元 0 的非零元.

8. 试给出有零因子环、无零因子环和整环的例子.

答 任意一个至少含两个元的循环加群 R，规定乘法运算为：$\forall a,b\in R, ab=0$. 于是 R 是一个有零因子环. 数集对于普通的数的加法和乘法来说作成的数环都是无零因子环. 零环 $\{0\}$、整数环都是整环.

9. 试判断下列各命题是否正确.

1） 把群 G 的代数运算叫加法，记为 $+$，则 G 为加群.

2） 设 $a,b,c\in$环 R，若 $a+b=a+c$，则 $b=c$.

3） 环 R 对于乘法来说作成一个群.

4） 设 G 是任意一个加群，那么一定可以对 G 规定一个乘法，使 G 作成一个环.

5） 在环中必存在元素与其他元素对于乘法来说可交换.

6） 环 R 中必有单位元.

7） 设 $x\in$环 R，则 $x^0\in R$，只要 $x\neq 0$.

8） 若环 R 有单位元，则环 R 至少有两个元.

9） 设环 R 有单位元 1，则 $1+1=2$.

10） 设环 R 有单位元 1，则 1 的负元 -1 等于 1.

11） 在有单位元的环中，零元永远没有逆元.

12） $\forall a\in$环 $R, a\neq 0$，a 必有逆元.

13） 设环 R 有单位元 1，$a\in R, a\neq 0$ 且 a 在 R 里有逆元，则 $a^{-1}\neq -a$.

14） 在任意一个环 R 里，$\forall a\in R$，a 的负整数次幂都有意义.

15） 设 R 是无零因子环，$x\in R$ 且 $3x=0$，则 $x=0$.

16） ① 环 R 里两个乘法消去律成立. 即：$\forall a,b,c\in R, a\neq 0$，有

左消去律 $ab=ac \Rightarrow b=c$,

右消去律 $ba=ca \Rightarrow b=c$.

② 在无零因子环 R 中，有 $ab=ac\Rightarrow b=c$.

17） 在恰有 n 个元的环 R 中，$\forall a\in R, na=0$.

答 1） 不正确. 加群对于加法来说必须作成一个交换群.

例 $G=\{0,a,b,c,d,e\}$对于加法

$+$	0	a	b	c	d	e
0	0	a	b	c	d	e
a	a	b	0	d	e	c
b	b	0	a	e	c	d
c	c	e	d	0	b	a
d	d	c	e	a	0	b
e	e	d	c	b	a	0

来说作成一个群. 但因 G 不是交换群，故 G 不是加群.

2） 正确. 因环 R 是加群，故加法消去律成立.

3） 不正确. 例，因整数环 $\mathbb{Z}$ 中的零元无逆元，故 $\mathbb{Z}$ 对于乘法来说不能作成一个群.

4） 正确. 规定：$\forall a,b\in G, ab=0$，于是 G 作成一个环.

5）　正确.因环中必有零元 0,而 0 与环中其他元素对于乘法来说都可交换.

6）　不正确.例,偶数环 $2\mathbb{Z}=\{2n|n\in\mathbb{Z}\}$无单位元.因为若$\exists e\in 2\mathbb{Z}$,使得$\forall 2n\in 2\mathbb{Z}$,$e2n=2ne=2n$,则必 $e=1$.但 $1\overline{\in}2\mathbb{Z}$,从而 $2\mathbb{Z}$ 无单位元.同理,当 k 是大于 1 的正整数时,$k\mathbb{Z}=\{kn|n\in\mathbb{Z}\}$也是无单位元环.

7）　不正确.因由定义 $x^0=1$,但环 R 未必有单位元 1.例,$2\in$偶数环 $2\mathbb{Z}$,但 $2^0\overline{\in}2\mathbb{Z}$,虽 $2\neq 0$.只要环 R 有单位元 1,必有 $x^0=1\in R$,不需条件 $x\neq 0$.

8）　不正确.例,零环$\{0\}$有单位元 0,但$\{0\}$只有一个元.可是我们有下面的结论:若环 R 有单位元 1,则 $0\neq 1\Leftrightarrow R$ 至少有两个元.

9）　不正确.应为 $1+1=2\cdot 1$(单位元 1 的 2 倍).例,环 $\mathbb{Z}_2=\{[0],[1]\}$有单位元 $1=[1]$,但 $1+1=[1]+[1]=2[1]=[2]=[0]\neq 2$.当 R 特殊是整数环时,有 $1+1=2$.

10）　不正确.例,环 $M_2(\mathbb{Q})=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\middle|a,b,c,d\in\mathbb{Q}\right\}$有单位元 $1=\begin{pmatrix}1&0\\0&1\end{pmatrix}$.但 1 的负元 $-1=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\neq 1$.当然也有可能 $-1=1$.例,$R=\{0,1\}$对于

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

来说作成一个有单位元 1 的环.因 $1+1=0$,故 $-1=1$.

11）　不正确.例,零环$\{0\}$有单位元 0.因 $0\cdot 0=0$,故零元 0 有逆元.若环 $R\neq\{0\}$,则零元没有逆元.

12）　不正确.例,偶数环无单位元,其中元就不可能有逆元.又例,数域 F 上的 2 阶矩阵环 $M_2(F)=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\middle|a,b,c,d\in F\right\}$虽有单位元$\begin{pmatrix}1&0\\0&1\end{pmatrix}$,但$\begin{pmatrix}1&2\\0&0\end{pmatrix}\left(\neq\begin{pmatrix}0&0\\0&0\end{pmatrix}\right)$也无逆元.

13）　不正确.由上面 10)中第 2 个例子可知,1 的逆元 $1^{-1}=1=-1$.又例,模 5 的剩余类环 $\mathbb{Z}_5=\{[0],[1],[2],[3],[4]\}$有单位元$[1]$.$[2]\neq[0]$,$[2]^{-1}=[3]$,$-[2]=[3]$,从而$[2]^{-1}=-[2]$.当然,可能 $a^{-1}\neq -a$.如$[4]\in\mathbb{Z}_5$,$[4]\neq[0]$,$[4]^{-1}=[4]$,$-[4]=[-4]=[1]$,于是$[4]^{-1}\neq -[4]$.

14）　不正确.因为 a 的负整数次幂如下定义:设 n 是正整数,$a^{-n}=(a^{-1})^n$.所以环 R 必须有单位元,且 a 得有逆元 $a^{-1}\in R$.例,数域 F 上的 2 阶矩阵环 $M_2(F)$中的元$\begin{pmatrix}1&1\\0&0\end{pmatrix}$的负整数次幂没有意义.

15）　不正确.例,模 3 的剩余类环 $\mathbb{Z}_3$是无零因子环,$[2]\in\mathbb{Z}_3$,且 $3[2]=[0]$,但$[2]\neq[0]$.

16）　①　不正确.例,在模 4 的剩余类环 $\mathbb{Z}_4$中,$[2]\neq[0]$,$[2][3]=[2][1]$,但$[3]\neq[1]$.需要加条件:R 是无零因子环.即:

环 R 无零因子 $\Leftrightarrow$ 环 R 里两个消去律成立.

进一步还有

R 是无零因子环 $\Leftrightarrow\forall a,b,c\in$环 R,$a\neq 0$,下面三条等价:

(i) $b=c$；(ii) $ab=ac$；(iii) $ba=ca$.

② 不正确.例,整数环$\mathbb{Z}$是无零因子环,$0\cdot 2=0\cdot 3$,但$2\neq 3$.注意,环中消去律与群中消去律的区别.

17) 正确.因环R是加群,故由第七章,三,1,7)知命题成立.

10. 证明:

1) 零元0是环R的单位元$\Leftrightarrow$环$R=\{0\}$.

2) 环R中零元0有逆元$\Leftrightarrow$环$R=\{0\}$.

证 1) ($\Rightarrow$) $\forall a\in R$,因0是R的单位元,故$0a=a$.又$0a=0$,从而$a=0$.所以,$R=\{0\}$.($\Leftarrow$) 因$0\cdot 0=0$,故0是R的单位元.

2) ($\Rightarrow$) (反证法) 若$R\neq\{0\}$,则由1)知0不是R的单位元1,从而$\forall a\in R$,$0a=0\neq 1$,即0无逆元,此与假设矛盾.所以$R=\{0\}$.($\Leftarrow$) 因$0\cdot 0=0$,故0有逆元0.

注 该命题的逆否命题为

1) 零元0不是环R的单位元$\Leftrightarrow$环$R\neq\{0\}$.

2) 环R中零元0无逆元$\Leftrightarrow$环$R\neq\{0\}$.

二、典型问题分析

1. 证明:设S是加群G的非空子集,则

1) S是G的子群$\Leftrightarrow$(i) $a,b\in S\Rightarrow a+b\in S$,

(ii) $a\in S\Rightarrow -a\in S$.

(这里$-a$是a在G中的负元)

2) S是G的子群$\Leftrightarrow$(iii) $a,b\in S\Rightarrow a-b\in S$.

证 1) ($\Rightarrow$)(i) $\forall a,b\in S$,因$S<G$,故$a+b\in S$.

(ii) ① S的零元$0'$就是G的零元0.因为$\forall a\in S$,在S中,$0'+a=a$;在G中,$0+a=a$,从而$0'+a=0+a$.因G是加群,消去律成立,故$0'=0\in S$.

② a在S里的负元a'就是a在G里的负元$-a$.因为:$a\in S$,由①知S的零元就是G的零元0,从而有$0=a'+a$.a当然在G中,从而有$0=(-a)+a$.因G是加群,故方程$y+a=0$在G中的解唯一.所以$a'=-a\in S$.(另一证法.已证明S的零元$0'$就是G的零元$0\in S$.$a\in S$,下面证明a在S里的负元a'就是a在G里的负元$-a$:$a'=a'+0=a'+(a+(-a))=(a'+a)+(-a)=0'+(-a)=0+(-a)=-a\in S$.)

($\Leftarrow$) $S\neq\varnothing$且$S\subset G$.

Ⅰ.由已知S对于G的加法封闭.

Ⅱ.结合律成立.

Ⅳ.S有零元:因$S\neq\varnothing$,故$\exists a\in S$,由已知$-a\in S$,从而$a+(-a)=0\in S$.

Ⅴ.$\forall a\in S$,由已知$\exists -a\in S$,使得$-a+a=0$.

所以$S<G$.

2) 只需证(i),(ii)$\Leftrightarrow$(iii).

($\Rightarrow$) $\forall a,b\in S$,由(ii),$-b\in S$,由(i),$a+(-b)=a-b\in S$,从而(iii)成立.

($\Leftarrow$) $\forall a\in S$,由(iii),$a-a=0\in S$,再由(iii),$0-a=-a\in S$,从而(ii)成立.

$\forall a,b\in S$，由(ii)，$-b\in S$，由(iii)，$a-(-b)=a+b\in S$，所以(i)成立.

2. $R=\{0,a,b,c\}$. 加法和乘法由以下两个表分别给定：

	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

	0	a	b	c
0	0	0	0	0
a	0	0	0	0
b	0	a	b	c
c	0	a	b	c

证明：R 作成一个环.

证　R 对于加法和乘法封闭. 对于加法来说，由第七章，二，11 知 R 与阶为 4 的非循环群(Klein 四元群)同构，且 R 也是一个群. 又阶为 4 的非循环群是交换群，从而 R 也是交换群. 所以 R 作成一个加群.

R 的乘法适合结合律：$\forall x,y,z\in R$，

$$x(yz)=(xy)z. \tag{1}$$

事实上，当 $x=0$ 或 $x=a$ 时，(1)的两端都是 0. 当 $x=b$ 或 $x=c$ 时，(1)的两端都是 yz. 这就讨论了所有的可能性，所以乘法结合律成立.

两个分配律都成立：$\forall x,y,z\in R$，

$$x(y+z)=xy+xz, \tag{2}$$

$$(y+z)x=yx+zx. \tag{3}$$

事实上，(2)的证明与(1)的证明一样，只看 $x=0$ 或 $x=a$ 和 $x=b$ 或 $x=c$ 的情况即可.

下面证明(3)成立.

①　$y=0$ 时，(3)的两端都等于 zx.

由加法适合交换律，$z=0$ 时，(3)也成立.

②　$y=a$ 时，$z=a$，则(3)的两端都等于 0；$z=b$ 或 c，则(3)的两端都等于 x.

由加法适合交换律，$z=a$ 时，(3)也成立.

③　$y=b$ 时，$z=b$ 或 c，则(3)的两端都等于 0.

因加法适合交换律，故 $z=b$ 时，(3)也成立.

④　$y=c$ 时，$z=c$，则(3)的两端都等于 0.

以上穷尽了各种可能情况，因此(3)成立.

所以 R 是一个环.

注　1)　证明乘法结合律 $x(yz)=(xy)z$，$\forall x,y,z\in R$，要验证 $C_4^1\cdot C_4^1\cdot C_4^1=4^3=64$ 个等式，比较麻烦. 因此要尽量寻找规律性. 同样证明右分配律(3)：$\forall x,y,z\in R$，$(y+z)x=yx+zx$，也要验证 64 个等式. 所以，我们也要利用运算的特点来简化验证过程. 验证(3)还可采用下面方法：

①　当 y 或 z 中有一个等于 0 时，(3)的两端显然相等.

②　当 $y=z$ 时，即 $y+z=0$，从而(3)的两端都等于 0.

③　当 $y\neq z$，且 $y\neq 0$，$z\neq 0$ 时，具体来说，有以下三种情况：

$$(a+b)x=cx=x,\quad ax+bx=0+x=x;$$

$$(a+c)x=bx=x,\quad ax+cx=0+x=x;$$

$$(b+c)x=ax=0,\quad bx+cx=x+x=0.$$

又 R 的加法适合交换律,所以 $\forall x,y,z\in R$,均有 $(y+z)x=yx+zx$.

下面再给出一个验证(3)的方法:

i) 当 $y+z=0$ 时,即 $y=z$,从而(3)的两端都等于 0.

ii) 当 $y+z=a$ 时,$y=0,z=a$ 或 $y=b,z=c$,从而(3)的两端都等于 0.

iii) 当 $y+z=b$ 时,$y=0,z=b$ 或 $y=a,z=c$,从而(3)的两端都等于 x.

iv) 当 $y+z=c$ 时,$y=0,z=c$ 或 $y=a,z=b$,从而(3)的两端都等于 x.

因 R 的加法适合交换律,故 $z+y$ 与 $y+z$ 的情况相同.所以 $\forall x,y,z\in R$,都有 $(y+z)x=yx+zx$.

2) 因含 1,2 和 3 个元的环对于加法来说都作成循环群,故由第九章,二,4,该题中的 R 是含元的个数最少的非交换环,而且 R 无单位元.

3. 证明:二项式定理

$$(a+b)^n=a^n+\binom{n}{1}a^{n-1}b+\cdots+b^n$$

在交换环 R 中成立,其中 n 是正整数.

证 对 n 作数学归纳法.

$n=1$ 时,$(a+b)^1=a^1+b^1$,等式成立.

假定 $n=k$ 时,

$$(a+b)^k=a^k+\binom{k}{1}a^{k-1}b+\cdots+\binom{k}{i}a^{k-i}b^i+\cdots+b^k.$$

下面证明 $n=k+1$ 时,等式也成立.

$$\begin{aligned}
&(a+b)^{k+1}=(a+b)^k(a+b)\\
&=\left(a^k+\binom{k}{1}a^{k-1}b+\cdots+\binom{k}{i}a^{k-i}b^i+\cdots+b^k\right)(a+b)\\
&\xlongequal[\text{分配律}]{\text{由 }ab=ba}a^{k+1}+\binom{k}{1}a^kb+\cdots+\binom{k}{i}a^{k-i+1}b^i+\cdots+ab^k+a^kb+\cdots+\binom{k}{i-1}a^{k-i+1}b^i+\cdots+\\
&\binom{k}{k-1}ab^k+b^{k+1}\\
&=a^{k+1}+\left[\binom{k}{1}+\binom{k}{0}\right]a^kb+\cdots+\left[\binom{k}{i}+\binom{k}{i-1}\right]a^{k-i+1}b^i+\cdots+\left[\binom{k}{k}+\binom{k}{k-1}\right]ab^k+b^{k+1}\\
&=a^{k+1}+\binom{k+1}{1}a^kb+\cdots+\binom{k+1}{i}a^{k+1-i}b^i+\cdots+\binom{k+1}{k}ab^k+b^{k+1}
\end{aligned}$$

(由 $\binom{k+1}{r}=\binom{k}{r}+\binom{k}{r-1}$,$0\leqslant r\leqslant k$)

根据归纳原理,对于任意正整数 n,等式都成立.

注 证明的关键是利用 a 与 b 可交换及分配律.不需 R 是交换环,只需 $ab=ba$.

4. 假定一个环 R 对于加法来说作成一个循环群.证明:R 是交换环.

证 设 $R=(a)=\{na\mid n\in\mathbb{Z}\}$.$\forall na,ma\in R$,有

$$(na)(ma)=n[a(ma)]=n[m(aa)]=(nm)a^2.$$

$$(ma)(na)=m[a(na)]=m[n(aa)]=(mn)a^2=(nm)a^2.$$

因此 $(na)(ma)=(ma)(na)$,从而 R 是交换环.

注 由该命题知,元的个数少于 4 的环必为交换环.

5. 证明:对于有单位元 1 的环 R 来说,加法适合交换律是环定义里其他条件的结果(利

用$(a+b)(1+1)$).

证　$\forall a,b\in R$,

$$(a+b)(1+1)\xlongequal{\text{左分配律}}(a+b)1+(a+b)1\xlongequal{\text{右分配律}}a1+b1+a1+b1=\!=a+b+a+b,$$

$$(a+b)(1+1)\xlongequal{\text{右分配律}}a(1+1)+b(1+1)\xlongequal{\text{左分配律}}a1+a1+b1+b1=\!=a+a+b+b,$$

从而

$$a+b+a+b=a+a+b+b.$$

因a,b有负元$-a,-b\in R$且R对加法封闭,故

$$(-a)+a+b+a+b+(-b)=(-a)+a+a+b+b+(-b).$$

由加法适合结合律及负元定义,

$$0+b+a+0=0+a+b+0.$$

由零元定义,$b+a=a+b$.所以加法适合交换律.

注　下面的证法是错误的:$\forall a,b\in R$,

$$(a+b)+[-(b+a)]=a+b-(b+a)=\!=a+b-b-a^{①}=0,$$

从而$a+b=-[-(b+a)]=b+a$.

因为证明中利用了$-(b+a)=-b-a$,而这个等式的证明却利用了加法交换律②.所以该命题中不可将R有单位元这一条件去掉.还可从下例来看:$G=\{0,a,b,c,d,e\}$对于加法

+	0	a	b	c	d	e
0	0	a	b	c	d	e
a	a	b	0	d	e	c
b	b	0	a	e	c	d
c	c	e	d	0	b	a
d	d	c	e	a	0	b
e	e	d	c	b	a	0

来说作成一个群(见第九章,一,9,1)).定义$\forall x,y\in G,xy=0$,则G满足环定义里除了加法交换律以外的所有条件.G无单位元.加法交换律不成立.G不是环.因此加法交换律独立于环定义里的其他条件.

6. 证明:由所有实数$a+b\sqrt{2}$(a,b是整数)作成的集合对于普通加法和乘法来说是一个整环.

证　设$R=\left\{a+b\sqrt{2}\,\middle|\,a,b\in\mathbb{Z}\right\}$.

1)　R是加群.事实上,因$0=0+0\sqrt{2}\in R$,故$R\neq\varnothing$.

Ⅰ.　R对加法封闭.$\forall a+b\sqrt{2},c+d\sqrt{2}\in R$,

$$(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+c)\sqrt{2}\in R$$

(因$a+c,b+c\in\mathbb{Z}$)且和唯一.

Ⅱ.　加法结合律和交换律都成立.因为R是实数集的一个子集,而实数的加法是可结

①②　张禾瑞.近世代数基础.北京:高等教育出版社,1978.81.(5)

合、可交换的.

Ⅳ. R 有零元 $0=0+0\sqrt{2}$.

Ⅴ. $\forall a+b\sqrt{2}\in R, a+b\sqrt{2}$ 有负元 $-(a+b\sqrt{2})=-a+(-b)\sqrt{2}\in R$,使得 $(a+b\sqrt{2})+(-a+(-b)\sqrt{2})=0+0\sqrt{2}$.

所以 R 是加群.

2) R 对乘法封闭. $\forall a+b\sqrt{2}, c+d\sqrt{2}\in R$,因 $ac+2bd, ad+bc\in\mathbb{Z}$,故 $(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}\in R$ 且积唯一.

3) 乘法结合律成立. 因为实数的乘法适合结合律.

4) 两个分配律成立. 因为实数满足乘法对于加法的分配律.

所以 R 是一个环. 又

1) 乘法适合交换律. 因为实数的乘法可交换.

2) R 有单位元 $1=1+0\sqrt{2}$.

3) R 没有零因子. 因为任意两个非零实数的乘积必不等于零.

所以 R 是一个整环.

注 1) 证明 R 是加群还可采用下面方法.

全体实数的集 $\mathbb{R}$ 对于普通加法来说作成一个加群. $R=\left\{a+b\sqrt{2}\,\middle|\,a,b\in\mathbb{Z}\right\}$ 是 $\mathbb{R}$ 的非空子集. $\forall a+b\sqrt{2}, c+d\sqrt{2}\in R$, $(a+b\sqrt{2})-(c+d\sqrt{2})=(a-c)+(b-d)\sqrt{2}\in R$,从而由子加群的判别条件,$R$ 是 $\mathbb{R}$ 的子加群. 所以 R 是加群.

2) 证明 R 无零因子还可利用以下方法.

$\forall a+b\sqrt{2}, c+d\sqrt{2}\in R$,若 $a+b\sqrt{2}\neq 0$,而 $(a+b\sqrt{2})\cdot(c+d\sqrt{2})=0$,则 $(ac+2bd)+(ad+bc)\sqrt{2}=0$,即

$$\begin{cases}ac+2bd=0\\ ad+bc=0.\end{cases}$$

因 $a+b\sqrt{2}\neq 0$,故 a,b 不全为 0,从而方程组

$$\begin{cases}cx+2dy=0\\ dx+cy=0\end{cases}$$

有非零解,于是其系数行列式 $\begin{vmatrix}c & 2d\\ d & c\end{vmatrix}=0$,即 $c^2-2d^2=0, c^2=2d^2, c=\pm\sqrt{2}d$. 因 c 为整数,$\sqrt{2}$ 为无理数,故 $d=0$,从而 $c=0$,因此 $c+d\sqrt{2}=0$. 所以 R 无零因子.

还可用下法证明 R 无零因子.

$\forall a+b\sqrt{2}, c+d\sqrt{2}\in R$,若 $a+b\sqrt{2}\neq 0$,而 $(a+b\sqrt{2})\cdot(c+d\sqrt{2})=0$,则

$$ac+2bd=0, \tag{4}$$

$$ad+bc=0. \tag{5}$$

从而 $abcd+2(bd)^2=0, abcd+(bc)^2=0$,即

$$2(bd)^2=(bc)^2. \tag{6}$$

① 若 $b=0$,由(4),$ac=0$. 因 $a+b\sqrt{2}\neq 0$,故 $a\neq 0$. 由 $\mathbb{Z}$ 无零因子,$c=0$. 再由(5),$d=0$. 于是 $c+d\sqrt{2}=0$.

② 若 $b\neq 0$，由(6)及 $\mathbb{Z}$ 中消去律成立，$2d^2=c^2$，即 $c=\pm\sqrt{2}d$. 因 $c\in\mathbb{Z}$，$\sqrt{2}$ 为无理数，故 $d=0$，从而 $c=0$，因此 $c+d\sqrt{2}=0$.

综上可知，R 无零因子.

三、讲与练

1. 首先给出定义：

设 R 是一个环. 若 $\exists e\in R$，使得 $\forall a\in R$，$ea=a(ae=a)$，则称 e 为 R 的左(右)单位元.

设 R 是一个有单位元 1 的环，$a\in R$. 若 $\exists a'\in R$，使得 $a'a=1(aa'=1)$，则称 a' 为 a 的左(右)逆元，称 a 为 R 中的左(右)可逆元.

试判断下面各命题是否正确.

1） 若环 R 有左单位元，则 R 有右单位元.

2） 环 R 的右零因子是 R 的左零因子.

3） 在有单位元 1 的环 R 中，

① 若 a 是可逆元，则 a 不是零因子.

② 左(右)可逆元不是左(右)零因子.

③ 若 a 是左(右)零因子，则 a 或者没有右(左)逆元，或者最少有两个右(左)逆元.

4） 在有单位元 1 的环 R 中，

① 若 a 不是零因子，则 a 是可逆元.

② 若 a 不是左(右)零因子，则 a 是左(右)可逆元.

③ 若 a 或者没有右(左)逆元，或者最少有两个右(左)逆元，则 a 是左(右)零因子.

5） 在有单位元 1 的环 R 中，a 的右逆元是 a 的左逆元.

6） 设 R 是无零因子环，则 R 的左(右)单位元是 R 的单位元.

7） 设 R 是有单位元 1 的环，R 无零因子. 若 $a(\in R)$ 有左(右)逆元，则 a 有右(左)逆元.

8） 在有单位元 1 的环 R 中，若 a 既有左逆元 a'，又有右逆元 a''，则 $a''=a'$.

解 1） 不正确. 例，$R=\left\{\begin{pmatrix}a&b\\0&0\end{pmatrix}\middle|\,a,b\in\mathbb{Q}\right\}$ 对于矩阵加法与乘法作成一个环. $\forall c\in\mathbb{Q}$，$\begin{pmatrix}1&c\\0&0\end{pmatrix}$ 都是 R 的左单位元，从而 R 有无穷多个左单位元. 但 R 无右单位元，因为对于 $\begin{pmatrix}0&1\\0&0\end{pmatrix}\in R$，$\forall\begin{pmatrix}a&b\\0&0\end{pmatrix}\in R$，$\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}a&b\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}\neq\begin{pmatrix}0&1\\0&0\end{pmatrix}$，所以 R 中的任意元都不是 R 的右单位元.

注 对称地，环 $R'=\left\{\begin{pmatrix}a&0\\b&0\end{pmatrix}\middle|\,a,b\in\mathbb{Q}\right\}$ 中，$\forall c\in\mathbb{Q}$，$\begin{pmatrix}1&0\\c&0\end{pmatrix}$ 都是 R' 的右单位元，从而 R' 有无穷多个右单位元. 但 R' 无左单位元.

2） 不正确. 例，在环 $R=\left\{\begin{pmatrix}a&b\\0&0\end{pmatrix}\middle|\,a,b\in\mathbb{Q}\right\}$ 中，$\forall c\in\mathbb{Q}$，$\begin{pmatrix}1&c\\0&0\end{pmatrix}$ 是 R 的右零因子，因为 $\exists d(\neq 0)\in\mathbb{Q}$，$\begin{pmatrix}0&d\\0&0\end{pmatrix}\in R$，使得 $\begin{pmatrix}0&d\\0&0\end{pmatrix}\begin{pmatrix}1&c\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$. 但 $\begin{pmatrix}1&c\\0&0\end{pmatrix}$ 不是 R 的左零因子，

因为$\forall \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in R, \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$,都有$\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

注 ① 对称地,在环$R' = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| a,b \in \mathbf{Q} \right\}$中,$\forall c \in \mathbf{Q}$,$\begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix}$是$R'$的左零因子,但不是右零因子.

② $M_2(\mathbf{Q}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d \in \mathbf{Q} \right\}$对于矩阵加法与乘法作成一个环. $\forall f \in \mathbf{Q}$, $\begin{pmatrix} 1 & f \\ 0 & 0 \end{pmatrix}$是$M_2(\mathbf{Q})$的右零因子,同时$\begin{pmatrix} 1 & f \\ 0 & 0 \end{pmatrix}$也是$M_2(\mathbf{Q})$的左零因子. 因为$\exists \begin{pmatrix} f & f \\ -1 & -1 \end{pmatrix} \left(\neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right) \in M_2(\mathbf{Q})$,使得$\begin{pmatrix} 1 & f \\ 0 & 0 \end{pmatrix}\begin{pmatrix} f & f \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. 同理$\forall f \in \mathbf{Q}$, $\begin{pmatrix} 1 & 0 \\ f & 0 \end{pmatrix}$是$M_2(\mathbf{Q})$的左零因子,也是右零因子.

③ 环的单位元显然不是零因子. 但环的左(右)单位元可能是右(左)零因子. 如环$\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a,b \in \mathbf{Q} \right\}$的左单位元$\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}(c \in \mathbf{Q})$是右零因子. 环$\left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| a,b \in \mathbf{Q} \right\}$的右单位元$\begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix}(c \in \mathbf{Q})$是左零因子. 显然左(右)单位元一定不是左(右)零因子.

3) ① 正确. 因a是可逆元,故$\exists a^{-1} \in R$,使得$a^{-1}a = 1$. $\forall b \in R$,若$ab = 0$,则$a^{-1}ab = a^{-1}0$,即$b = 0$,从而a不是零因子.

② 正确. 事实上,设a是左可逆元,则$\exists a' \in R$,使得$a'a = 1$. 假定a是左零因子,则$\exists b \in R, b \neq 0$,使得$ab = 0$,从而$a'ab = a'0$. 于是$1b = 0$,即$b = 0$,产生矛盾. 所以$a$不是左零因子. 同理可证右可逆元不是右零因子.

③ 正确. 因已知a是左零因子,即$\exists b(\neq 0) \in R$,使得$ab = 0$. 如果a没有右逆元,那么命题已成立. 如果a有右逆元a',使$aa' = 1$. 因$aa' + ab = 1 + ab, ab = 0$,故$a(a' + b) = 1$,从而$a' + b$是$a$的一个右逆元. 因$b \neq 0$,故$a' + b \neq a'$,所以$a$最少有两个右逆元$a'$与$a' + b$. 类似地可证明另一情况.

注 该命题的逆否命题成立. 即:设R是有单位元1的环,则

① R的零因子一定不是可逆元.

② R的左(右)零因子一定不是左(右)可逆元.

③ 如果$a(\in R)$有唯一的一个右(左)逆元,那么a不是左(右)零因子.

4) ① 不正确. 例,整数环$\mathbf{Z}$是有单位元1的环. $2(\in \mathbf{Z})$不是零因子,但2也不是可逆元.

② 不正确. $2(\in \mathbf{Z})$不是左(右)零因子,但2也不是左(右)可逆元.

③ 不正确. $2(\in \mathbf{Z})$没有右(左)逆元,但2也不是左(右)零因子.

注 命题4)说明命题3)的逆命题不成立.

5) 不正确. 例,设F是数域,F_∞是所有形如

$$\begin{pmatrix} a_{11} & a_{12} & \cdots \\ a_{21} & a_{22} & \cdots \\ \vdots & \vdots & \end{pmatrix}$$

$(a_{ij} \in F)$的无限阶矩阵所作成的集,其中,每一列和每一行都只有有限多个元$\neq 0$. 规定F_∞

的＋和·分别为矩阵加法和乘法. 则 F_∞ 作成一个有单位元的环,此单位元是主对角线上的元素都是 1,其他元素都是 0 的矩阵.

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & \ddots \end{pmatrix}$$

设

$$a=\begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & 0 & 1 & \\ & & & \ddots & \ddots \end{pmatrix},\quad b=\begin{pmatrix} 0 & & & \\ 1 & 0 & & \\ & 1 & 0 & \\ & & 1 & \ddots \\ & & & \ddots \end{pmatrix}.$$

$a(b)$ 中与主对角线相邻的右(左)上(下)斜线上的元素为 1,其余的元素都是 0.

因 $ab=\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & \ddots \end{pmatrix}$,故 b 是 a 的右逆元. 但 $ba\neq\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & \ddots \end{pmatrix}$,故 b 不是 a 的左逆元. 实际上,a 有右逆元,但 a 无左逆元. 因为 $\exists\, c=\begin{pmatrix} 1 & & & \\ & 0 & & \\ & & 0 & \\ & & & \ddots \end{pmatrix}(\neq 0)\in F_\infty$,使得 $ac=0$,从而 a 是 F_∞ 的左零因子,由上面题 1、3),②知,a 无左逆元.

注　该例中,b 有左逆元 a,但 b 无右逆元. a 是左零因子,但不是右零因子. b 是右零因子,但不是左零因子.

6)　正确. 事实上,若 $R=\{0\}$,则命题显然成立. 若 $R\neq\{0\}$,设 e 是 R 的左单位元,显然 $e\neq 0$ 且 $ee=e$. 于是 $\forall\, a\in R$,$aee=ae$,即 $(ae-a)e=0$. 因 R 无零因子,$e\neq 0$,故 $ae-a=0$,即 $ae=a$,从而 e 也是右单位元. 因此 e 是单位元. 同理 R 的右单位元也是左单位元,因此是单位元.

注　由证明可见,条件减弱为:R 是没有右零因子的环或 R 是没有左零因子的环,结论也成立.

7)　正确. 事实上,若 $R=\{0\}$,命题显然成立. 若 $R\neq\{0\}$,设 a' 是 a 的左逆元,则 $a'\neq 0$,$a'a=1$. 于是 $a'aa'=1a'=a'1$,即 $a'(aa'-1)=0$. 因 $a'\neq 0$,R 无零因子,故 $aa'-1=0$,即 $aa'=1$,从而 a' 也是 a 的右逆元. 类似地可证,若 a 有右逆元,则 a 有左逆元.

注　条件减弱为:R 无左零因子或 R 无右零因子时,结论也成立.

8)　正确. 事实上,因 $a'a=1$,$aa''=1$,故 $a''=1a''=(a'a)a''=a'(aa'')=a'1=a'$.

2. 若环 R 有且只有一个左(右)单位元 e,证明:e 必为 R 的右(左)单位元.

证一　(反证法)假设 R 的左单位元 e 不是 R 的右单位元,则 $\exists\, x\in R$,使得 $xe\neq x$,从而 $xe-x\neq 0$,即 $xe-x+e\neq e$. $\forall\, a\in R$,

$$(xe-x+e)a=xea-xa+ea=xa-xa+a=a.$$

说明 $xe-x+e$ 是 R 的一个左单位元,但 $xe-x+e\neq e$,此与已知矛盾. 所以 e 是 R 的右单位元. 类似地可证,环 R 的唯一的右单位元也是 R 的左单位元.

证二　已知 e 是 R 的左单位元,即 $\forall\, a\in R$,$ea=a$. $\forall\, b\in R$,

$$(ae-a+e)b=aeb-ab+eb=ab-ab+b=b.$$

说明 $ae-a+e$ 是 R 的左单位元,又左单位元唯一,从而 $ae-a+e=e$,即 $ae-a=0$,$ae=a$,

$\forall a\in R$.所以 e 是 R 的右单位元.同理可证另一情况.

注 命题的逆否命题是:若 $e(\in$环 $R)$不是 R 的右(左)单位元,且 e 是 R 的左(右)单位元,则 R 有不只一个左(右)单位元.

3. 在有单位元 1 的环 R 中,若 a 有唯一的左(右)逆元,证明:a 是可逆元.

证一 (反证法) 假设 a 不是可逆元.已知 a 是一个左可逆元.从而 $\exists a'\in R$,使得 $a'a=1$,即 a'是 a 的左逆元.但 a'不是 a 的右逆元,即 $aa'\neq 1$,于是 $aa'-1\neq 0$,$a'+aa'-1\neq a'$.因

$$(a'+aa'-1)a=a'a+aa'a-a=1+a1-a=1.$$

故 $a'+aa'-1$ 也是 a 的一个左逆元.但 $a'+aa'-1\neq a$,此与已知矛盾.所以 a 是可逆元.另一情况类似可证.

证二 因 a 有左逆元,故 $\exists a'\in R$,使得 $a'a=1$,从而

$$(a'+aa'-1)a=a'a+aa'a-a=1+a1-a=1.$$

于是 $a'+aa'-1$ 是 a 的一个左逆元.因 a 的左逆元唯一,故 $a'+aa'-1=a'$,即 $aa'-1=0$,$aa'=1$.所以 a'也是 a 的右逆元.因此 a'是 a 的逆元,a 是可逆元.同理可证另一情况.

证三 若 $R=\{0\}$,命题显然成立.若 $R\neq\{0\}$,因 a 有左逆元 a',故 $a'a=1$,且 $a\neq 0$.从而 $aa'a=a1=1a$,即$(aa'-1)a=0$.已知 a 有唯一的左逆元,由上面题 1,3),③知 a 不是右零因子.又 $a\neq 0$,于是 $aa'-1=0$,即 $aa'=1$.所以 a'也是 a 的右逆元.因此 a'是 a 的逆元,即 a 是可逆元.若 a 有唯一的右逆元,结论同理可证.

注 设 R 是有单位元 1 的环.$a(\in R)$不是可逆元,但 a 有左(右)逆元,则 a 有不只一个左(右)逆元.

4. 设环 R 有单位元 $1\neq 0$,$a\in R$,a 有右逆元.证明下面各命题等价.

1) a 有不只一个右逆元;

2) a 没有左逆元;

3) a 是一个左零因子.

证一 1)$\Rightarrow$3):因 a 有不只一个右逆元,故 $\exists a',a''\in R$,$a'\neq a''$,a',a''都是 a 的右逆元,即 $aa'=1$,$aa''=1$,且 $a\neq 0$,从而 $aa'=aa''$,即 $a(a'-aa'')=0$ 且 $a'-a''\neq 0$.又 $a\neq 0$,于是 a 是一个左零因子.

3)$\Rightarrow$2):见上面题 1,3),②.

2)$\Rightarrow$1):见上面题 3.

证二 1)$\Rightarrow$2):(反证法)若 a 有左逆元 a',$a'a=1$.已知 a 至少有两个右逆元 a_1,a_2,$aa_1=1$,$aa_2=1$,于是

$$a_1=1a_1=(a'a)a_1=a'(aa_1)=a'1=a',$$
$$a_2=1a_2=(a'a)a_2=a'(aa_2)=a'1=a',$$

从而 $a_1=a_2$,此与已知矛盾.所以 a 无左逆元.

2)$\Rightarrow$3):因 a 有右逆元 a',故 $aa'=1$,且 $a\neq 0$.因 a 无左逆元,故 $a'a\neq 1$,即 $a'a-1\neq 0$.但

$$a(a'a-1)=aa'a-a=1a-a=0,$$

且 $a\neq 0$,从而 a 是一个左零因子.

3)$\Rightarrow$1):见上面题 1,3),③.

注 将该命题中的"右"改为"左","左"改为"右"以后,结论也成立.

5. 设环 R 有单位元 1,$a\in R$,a 的右逆元多于一个,求证:a 有无限多个右逆元.

证一　作集 $S=\left\{s\in R \middle| s\text{ 是 }a\text{ 的右逆元,即 }as=1\right\}$,则 S 中至少有 2 个元.取定 $s_0\in S$.再作集 $K=\left\{sa-1+s_0 \middle| s\in S\right\}$,因为 $\forall k=sa-1+s_0\in K$,

$$ak=a(sa-1+s_0)=asa-a+as_0=1a-a+1=1.$$

所以 $k\in S$,因此 $K\subset S$.因 a 有不只一个右逆元,故由上面题 4,a 没有左逆元,从而 $\forall s\in S$,$sa\neq 1$,即 $sa-1\neq 0$,$sa-1+s_0\neq s_0$.于是 $s_0\overline{\in} K$,因此 K 是 S 的真子集.令 $\phi: s\to sa-1+s_0$,显然 ϕ 是 S 到 K 的一个满射.$\forall s,t\in S$,若 $\phi(s)=\phi(t)$,即 $sa-1+s_0=ta-1+s_0$,则 $sa=ta$.于是 $sas_0=tas_0$,从而 $s1=t1$,即 $s=t$,因此 ϕ 是单射.所以 ϕ 是 S 与 K 间的一个一一映射.因 K 是 S 的真子集,故 S 是无限集,从而 a 有无限多个右逆元.

证二　(反证法)假设 a 只有有限多个右逆元.若 a 恰有 n 个互不相同的右逆元:$a_1,a_2,\cdots,a_n$,则 $aa_i=1(i=1,2,\cdots,n)$.令

$$k_i=a_ia-1+a_1,\ i=1,2,\cdots,n.$$

因

$$ak_i=a(a_ia-1+a_1)=aa_ia-a1+aa_1=1a-a+1=1,$$

故 $k_i(i=1,2,\cdots,n)$ 也是 a 的右逆元.当 $i\neq j$ 时,若 $k_i=k_j$,即 $a_ia-1+a_1=a_ja-1+a_1$,从而 $a_ia=a_ja$,两边都右乘 a_1,得 $a_iaa_1=a_jaa_1$,即 $a_i1=a_j1$.于是 $a_i=a_j(i\neq j)$,矛盾.所以,当 $i\neq j$ 时,$k_i\neq k_j$.即 $k_1,k_2,\cdots,k_n$ 是 a 的互不相同的 n 个右逆元.又 $k_i\neq a_1(i=1,2,\cdots,n)$,事实上,假设 $k_i=a_1$,即 $a_ia-1+a_1=a_1$,从而 $a_ia=1$.因此 a 有左逆元 a_i,但 a 至少有两个右逆元.此与上面题 4 矛盾,从而 $k_i\neq a_1$.于是 $a_1,k_1,k_2,\cdots,k_n$ 是 a 的 $n+1$ 个互不相同的右逆元.此与 a 恰有 n 个互不相同的右逆元矛盾.所以 a 有无限多个右逆元.

注　命题中,“右”改为“左”,结论仍成立.

6. 证明:任意一个不仅含一个数的有限数集 A 对于普通加法与乘法来说不能作成一个环.

证　(反证法)设 A 是一个环.因 A 不仅含一个数,故 $\exists a\in A$,使得 $a\neq 0$.因 A 是环,故 $a,2a,\cdots,na,\cdots\in A$,其中 n 是正整数.因 $a\neq 0$,故当 m 与 n 是两个不同的正整数时,$ma\neq na$,于是 A 中有无限多个数,此与 A 是有限数集矛盾.所以 A 不能作成环.

7. 设 R 是一个环,整数 $n\geq 1$.

$$M_n(R)=\{A\mid A\text{ 是元在环 }R\text{ 中的 }n\text{ 阶矩阵}\}$$

与通常矩阵一样地定义 $M_n(R)$ 的加法与乘法,则 $M_n(R)$ 作成一个环.称 $M_n(R)$ 为环 R 上 n 阶全矩阵环.证明:

1)　当环 R 有单位元 1 时,环 $M_n(R)$ 也有单位元.

2)　若环 $R\neq\{0\}$,$n>1$,则 $M_n(R)$ 有零因子.

3)　若 $\exists a,b\in R$,使得 $ab\neq 0$,$n>1$,则 $M_n(R)$ 非交换.

证　1)　显然 $\begin{pmatrix}1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1\end{pmatrix}$ 是 $M_n(R)$ 的单位元.

2)　因 $R\neq\{0\}$,故 $\exists a\in R$,$a\neq 0$.取

$$A=\begin{pmatrix}a & 0 & \cdots & 0\\ 0 & 0 & \cdots & 0\\ \vdots & \vdots & & \vdots\\ 0 & 0 & \cdots & 0\end{pmatrix},\quad B=\begin{pmatrix}0 & 0 & \cdots & 0\\ 0 & 0 & \cdots & 0\\ \vdots & \vdots & & \vdots\\ 0 & 0 & \cdots & a\end{pmatrix}\in M_n(R),$$

从而 $A\neq0,B\neq0$,但 $AB=BA=0$,所以 A,B 是 $M_n(R)$的零因子.

3) 因 $ab\neq0$,故 $a\neq0$ 且 $b\neq0$. 取

$$C=\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},\quad D=\begin{pmatrix} 0 & b & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}\in M_n(R),$$

则

$$CD=\begin{pmatrix} 0 & ab & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}\neq0.$$

而 $DC=0$,因此 $CD\neq DC$. 所以 $M_n(R)$非交换.

注 1) 虽 R 为交换环,但 $M_n(R)$可能为非交换环. 例,$\mathbb{Z}_2$是交换环,零元 $0=[0]$,单位元 $1=[1]$. 取 $\begin{pmatrix}1&0\\0&0\end{pmatrix}$,$\begin{pmatrix}0&1\\0&0\end{pmatrix}\in M_2(\mathbb{Z}_2)$,$\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix}=\begin{pmatrix}0&1\\0&0\end{pmatrix}$,$\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}1&0\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$,因此,$\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix}\neq\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}1&0\\0&0\end{pmatrix}$. 所以,$M_2(\mathbb{Z}_2)$为非交换环.

2) 虽 R 为无零因子环,但 $M_n(R)$可能为有零因子环. 例,$\mathbb{Z}_2$是无零因子环,取 $\begin{pmatrix}1&0\\0&0\end{pmatrix}$,$\begin{pmatrix}0&0\\0&1\end{pmatrix}\in M_2(\mathbb{Z}_2)$,$\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&0\\0&1\end{pmatrix}=\begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix}1&0\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$. 所以,$\begin{pmatrix}1&0\\0&0\end{pmatrix}$,$\begin{pmatrix}0&0\\0&1\end{pmatrix}$是 $M_2(\mathbb{Z}_2)$的零因子.

8. 设 F 是数域,$A\in M_n(F)$,$A\neq0$,证明:

$$A\text{ 是 }M_n(F)\text{的零因子}\Leftrightarrow A\text{ 不是可逆矩阵}.$$

证一 由《高等代数》[1](第四章习题 14)知:设 $A\in M_n(F)$,$A\neq0$,则

$$\left.\begin{array}{l}\exists B\in M_n(F),B\neq0,\text{使得 }AB=0\\ \text{且 }\exists C\in M_n(F),C\neq0,\text{使得 }CA=0\end{array}\right.\Leftrightarrow A\text{ 不是可逆矩阵}.$$

下面我们来证明这个命题.

($\Rightarrow$) 已知 $A\in M_n(F)$,$\exists B\in M_n(F)$,$B\neq0$,使得 $AB=0$. 设 $B=(\beta_1,\beta_2,\cdots,\beta_n)$,其中 $\beta_1,\beta_2,\cdots,\beta_n$ 是 B 的列向量. 因 $B\neq0$,故不妨设 $\beta_1\neq0$. 因 $AB=0$,故$(A\beta_1,A\beta_2,\cdots,A\beta_n)=0$. 从而 $A\beta_1=0$,于是齐次线性方程组 $AX=0$ 有非零解 β_1,所以$|A|=0$,因此 A 不是可逆矩阵.

($\Leftarrow$) 已知 $A\in M_n(F)$,且 A 不是可逆矩阵,即$|A|=0$. 于是齐次线性方程组 $AX=0$ 有非零解 $\beta_1=\begin{pmatrix}b_1\\b_2\\\vdots\\b_n\end{pmatrix}$. 取 $B=\begin{pmatrix}b_1&0&\cdots&0\\b_2&0&\cdots&0\\\vdots&\vdots&&\vdots\\b_n&0&\cdots&0\end{pmatrix}\in M_n(F)$,则 $B\neq0$ 且使 $AB=0$.

下面我们再证明,当$|A|=0$ 时,也$\exists C\in M_n(F)$,$C\neq0$,使得 $CA=0$. 因$(CA)'=A'C'$,

[1] 北京大学数学系几何与代数教研室. 高等代数. 北京:高等教育出版社,1978

故只需证明$A'C'=0$. 因$|A'|=|A|=0$,故齐次线性方程组$A'X=0$有非零解$v_1=\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix}$. 令

$D=\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ d_2 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ d_n & 0 & \cdots & 0 \end{pmatrix}\in M_n(F)$,则 $D\neq 0$ 且使 $A'D=0$. 取 $C=D'\in M_n(F)$,于是 $C\neq 0$,且 $C'=D$,即 $A'C'=0$,从而 $CA=(A'C')'=0$.

所以由零因子定义,立即有:设 $A\in M_n(F)$,$A\neq 0$,则

$$A\text{ 是 }M_n(F)\text{的零因子}\Leftrightarrow A\text{ 不是可逆矩阵}.$$

证二 ($\Rightarrow$) (反证法) 若 A 是可逆矩阵,则$\exists A^{-1}\in M_n(F)$. 已知 A 是 $M_n(F)$的零因子,从而$\exists B\in M_n(F)$,$B\neq 0$,使得 $AB=0$,于是 $A^{-1}AB=A^{-1}0$,即 $B=0$,矛盾. 所以 A 不是可逆矩阵.(见上面题 1,3),①)

($\Leftarrow$) 已知 A 不是可逆矩阵,即$|A|=0$. 又 $A\neq 0$,从而 $0<$秩 $A=r<n$. 于是$\exists$可逆矩阵 $P,Q\in M_n(F)$,使得 $PAQ=\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix}$ (r个) $=D_r$(矩阵中主对角线外的元素都是 0),用

$H=\begin{pmatrix} 0 & & & \\ & \ddots & & \\ & & 0 & \\ & & & 1 \end{pmatrix}$($\in M_n(F)$,矩阵中主对角线外的元素都是 0),右乘上式两边,得 $PAQH=D_rH=0$,用 P^{-1}左乘上式两边,得 $AQH=0$,其中 $QH\neq 0$. 事实上,若 $QH=0$,因 Q 可逆,故$\exists Q^{-1}\in M_n(F)$,使得 $Q^{-1}QH=Q^{-1}0$,即 $H=0$,矛盾. 从而 $QH\neq 0$,所以 A 是$M_n(F)$的左零因子,再用 H 左乘 $PAQ=D_r$ 两边,得 $HPAQ=HD_r=0$. 因 Q 可逆,故 $HPA=0$. 因 P 可逆,$H\neq 0$,故 $HP\neq 0$. 所以 A 是 $M_n(F)$的右零因子. 于是 A 是 $M_n(F)$的零因子.

注 1) 设 F 是数域,$n>1$,则 n 阶全矩阵环 $M_n(F)$有零因子.

2) 所有的非零不可逆的数域 F 上 n 阶矩阵就是 $M_n(F)$的所有的零因子. 因此环 $M_n(F)$的零因子完全被刻划清楚了.

3) 在 $M_n(F)$中没有左、右零因子之分. 但 $M_n(F)(n>1)$非交换.

4) 在该命题中,若将数域 F 改为整环,则结论不成立. 例,在 $M_2(\mathbb{Z})$中,取 $A=\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$,则 A 不是可逆矩阵,但 A 不是 $M_2(\mathbb{Z})$的零因子. 因为$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix}(\neq 0)\in M_2(\mathbb{Z})$,

$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} 2a & 2b \\ 3c & 3d \end{pmatrix}\neq 0$,所以 A 不是左零因子,从而 A 不是零因子.

9. 设 R 是定义在实数集$\mathbf{R}$上的所有实函数的集. $\forall f,g\in R$,$\forall x\in\mathbf{R}$,规定

$$(f+g)(x)=f(x)+g(x),\quad (fg)(x)=f(x)g(x).$$

证明:

1) R 是交换环;

2) R 有零因子.

证 1) $\forall f,g\in R$，$\exists|$实函数 $f+g\in R$，从而 R 对$+$封闭.

$\forall f,g,h\in R$，$\forall x\in\mathbf{R}$，由数的加法适合结合律，有

$$\begin{aligned}[(f+g)+h](x) &= (f+g)(x)+h(x) = (f(x)+g(x))+h(x)\\ &= f(x)+(g(x)+h(x)) = f(x)+(g+h)(x) = [f+(g+h)](x),\end{aligned}$$

从而$(f+g)+h=f+(g+h)$.

$\forall f,g\in R$，$\forall x\in\mathbf{R}$，由数的加法适合交换律，有

$$(f+g)(x) = f(x)+g(x) = g(x)+f(x) = (g+f)(x),$$

从而 $f+g=g+f$.

$\exists$零函数 $0\in R$，$\forall x\in\mathbf{R}$，$0(x)=0$，使得$\forall f\in R$，有

$$(f+0)(x) = f(x)+0(x) = f(x),$$

即 $f+0=f$，从而 0 是 R 的零元.

$\forall f\in R$，$\exists f$ 的负函数$-f\in R$，$\forall x\in R$，$(-f)(x)=-f(x)$，使得

$$(f+(-f))(x) = f(x)+(-f)(x) = f(x)+(-f(x)) = f(x)-f(x) = 0 = 0(x),$$

即 $f+(-f)=0$，从而$-f$ 是 f 的负元.

所以 R 是一个加群.

$\forall f,g\in R$，$\exists|$实函数 $fg\in R$，从而 R 对 · 封闭.

$\forall f,g,h\in R$，$\forall x\in\mathbf{R}$，由数的乘法适合结合律，有

$$\begin{aligned}[(fg)h](x) &= (fg)(x)h(x) = (f(x)g(x))h(x)\\ &= f(x)(g(x)h(x)) = f(x)(gh)(x) = [f(gh)](x),\end{aligned}$$

从而$(fg)h=f(gh)$.

$\forall f,g,h\in R$，$\forall x\in\mathbf{R}$，由数的乘法对加法的分配律成立，得

$$\begin{aligned}[f(g+h)](x) &= f(x)[(g+h)(x)] = f(x)[g(x)+h(x)]\\ &= f(x)g(x)+f(x)h(x) = (fg)(x)+(fh)(x) = (fg+fh)(x),\end{aligned}$$

从而 $f(g+h)=fg+fh$. 同理$(g+h)f=gf+hf$.

综上所述，R 是一个环.

$\forall f,g,\in R$，$\forall x\in\mathbf{R}$，由数的乘法适合交换律，知

$$(fg)(x) = f(x)g(x) = g(x)f(x) = (gf)(x),$$

从而 $fg=gf$. 所以 R 是一个含有无限多个元的交换环，称为实数域$\mathbf{R}$上的全实函数环.

2) 令

$$f(x) = \begin{cases}0, & x\leqslant 1\\ 1, & x>1\end{cases},\quad g(x) = \begin{cases}1, & x\leqslant 1\\ 0, & x>1\end{cases}.$$

显然 $f,g\in R$，$f\neq 0$，$g\neq 0$，$fg,gf\in R$，$\forall x\in\mathbf{R}$，

$$(fg)(x) = (gf)(x) = 0 = 0(x),$$

从而 $fg=gf=0$，所以 f,g 都是R 的零因子.

注 1) 定义在闭区间$[a,b]$上的所有实函数的集对于普通的函数的加法与乘法(见该命题)来说也作成一个交换环，称为$[a,b]$上的全实函数环.

2) 在该命题中，将实函数分别改成连续实函数、可微实函数与可积实函数时，R 仍作成一个交换环.

3) 该命题可推广为如下形式：设 S 为非空集，K 是环，R 表示定义在 S 上而取值在 K

内的所有函数作成的集合，即 R 为集 S 到环 K 的所有映射作成的集合. 定义：$\forall f,g\in R$，$\forall x\in S$，

$$(f+g)(x)=f(x)+g(x),\quad (fg)(x)=f(x)g(x).$$

则 R 作成一个环，称 R 为集 S 上的取值在环 K 内的全函数环.

当 $S=K=\mathbf{R}$ 时，推广的命题即为原来命题.

当 K 是交换环时，R 也是交换环.

当集 S 至少有两个元，环 $K\neq\{0\}$ 时，环 R 有零因子. 事实上，因 $K\neq\{0\}$，故 $\exists k\in K$，$k\neq 0$. 由 S 至少有两个元，$\exists a,b\in S,a\neq b$. 令 $A=\{a\},B=S-A$，于是 $b\in B,B\neq\varnothing$ 且 $A\cap B=\varnothing,A\cup B=S$. 取

$$f(x)=\begin{cases}k, & x\in A\\ 0, & x\in B\end{cases},\quad g(x)=\begin{cases}0, & x\in A\\ k, & x\in B\end{cases}.$$

显然，$f,g,fg,gf\in R,f\neq 0,g\neq 0$，但 $fg=gf=0$. 所以 f,g 都是 R 的零因子.

当 $S=K$ 时，R 是环 K 的所有变换作成的环.

4)　在该命题中，若将乘法改为：

$$(fg)(x)=f(g(x)),$$

则 R 不作成环. 因为左分配律不成立. 例如，取 $f(x)=x^2,g(x)=2,h(x)=x$，于是

$$\begin{aligned}[f(g+h)](x)&=f[(g+h)(x)]=f[g(x)+h(x)]\\&=f(2+x)=(2+x)^2.\end{aligned}$$

但

$$\begin{aligned}(fg+fh)(x)&=(fg)(x)+(fh)(x)=f(g(x))+f(h(x))\\&=f(2)+f(x)=2^2+x^2=4+x^2.\end{aligned}$$

因此 $f(g+h)\neq fg+fh$. 容易验证右分配律与乘法结合律成立. 而且我们看出，想使左分配律成立，只需

$$f[g(x)+h(x)]=f(g(x))+f(h(x)).$$

因 $g(x),h(x)\in\mathbf{R}$，故只需，$\forall x_1,x_2\in\mathbf{R}$，

$$f(x_1+x_2)=f(x_1)+f(x_2).$$

从而启发我们考虑当 f 是 $\mathbf{R}$ 的自同态时，能否使 R 作成环呢？我们推广成下题.

10. 设 G 是加群，E 是 G 到 G 的所有自同态作成的集. 规定：$\forall f,g\in E,\forall x\in G$，

$$(f+g)(x)=f(x)+g(x),\quad (fg)(x)=f(g(x)).$$

证明：E 作成一个环.

证　$\forall f,g\in E$，显然 $f+g$ 是加群 G 到 G 的一个映射. 又 $\forall x_1,x_2\in G$，有

$$\begin{aligned}(f+g)(x_1+x_2)&=f(x_1+x_2)+g(x_1+x_2)=(f(x_1)+f(x_2))+(g(x_1)+g(x_2))\\&=(f(x_1)+g(x_1))+(f(x_2)+g(x_2))=(f+g)(x_1)+(f+g)(x_2),\end{aligned}$$

从而 $f+g$ 是 G 的自同态，所以 $\exists| f+g\in E$，即 E 对 $+$ 封闭. 与上面题 9 中的证明类似，可证 E 是一个加群. 进一步可证明 E 对乘法封闭(见第二章，二，5)，乘法适合结合律，乘法对加法的左、右分配律都成立. 所以 E 作成一个环. 称 E 为加群 G 的自同态环.

注　设 R 是环，E 是环 R 到 R 的所有自同态作成的集. 规定：$\forall f,g\in E,x\in R$，

$$(f+g)(x)=f(x)+g(x),\quad (fg)(x)=f(g(x)),$$

则 E 不作成环. 事实上，$\forall f,g\in E,\forall x_1,x_2\in E$，

$$(f+g)(x_1x_2)=f(x_1x_2)+g(x_1x_2)=f(x_1)f(x_2)+g(x_1)g(x_2),$$

但

$$(f+g)(x_1)\cdot(f+g)(x_2)=[f(x_1)+g(x_1)][f(x_2)+g(x_2)]$$
$$=f(x_1)f(x_2)+f(x_1)g(x_2)+g(x_1)f(x_2)+g(x_1)g(x_2),$$

从而

$$(f+g)(x_1x_2)\neq(f+g)(x_1)\cdot(f+g)(x_2).$$

所以环的两个自同态 f,g 的和 $f+g$ 一般不再是环的自同态. 因此 E 不作成环.

例 $f:a+bi\to a+bi, g:a+bi\to a-bi$ 是复数环 $\mathbb{C}$ 的两个自同态，但 $f+g$ 不是 $\mathbb{C}$ 的自同态.

11. 设 $\mathbb{Z}_n$ 是模 n 的剩余类环，$a\in$ 整数集 $\mathbb{Z}$，$1\leqslant a<n$，证明：

1) $[a]$ 是 $\mathbb{Z}_n$ 的可逆元 $\Leftrightarrow (a,n)=1$.

2) $[a]$ 是 $\mathbb{Z}_n$ 的零因子 $\Leftrightarrow (a,n)\neq 1$.

证 1) ($\Rightarrow$) 因 $[a]$ 是 $\mathbb{Z}_n$ 的可逆元，故 $\exists [b]\in\mathbb{Z}_n$，使得 $[b][a]=[1]$，即 $[ba]=[1]$，从而 $n\mid ba-1$. 于是 $\exists q\in\mathbb{Z}$，使得 $ba-1=nq$，即 $ba-nq=1$，所以 $(a,n)=1$.

($\Leftarrow$) 因 $(a,n)=1$，故 $\exists u,v\in\mathbb{Z}$，使得 $ua+vn=1$，即 $[u][a]+[v][n]=[1]$. 因 $[n]=[0]$，故 $[u][a]=[1]$ 且 $[a][u]=[1]$，从而 $[a]^{-1}=[u]$. 所以 $[a]$ 是 $\mathbb{Z}_n$ 的可逆元.

2) ($\Leftarrow$) 设 $(a,n)=d\neq 1$，则 $\exists a_1,n_1\in\mathbb{Z}$，使得 $a=da_1, n=dn_1$. 因 $1\leqslant a<n$，故 $[a]\neq[0]$. 因 $1\leqslant n_1<n$，故 $[n_1]\neq[0]$. 又

$$[a][n_1]=[an_1]=[da_1n_1]=[a_1n]=[a_1][n]=[0].$$

同理，$[n_1][a]=[0]$，所以 $[a]$ 是 $\mathbb{Z}_n$ 的零因子.

($\Rightarrow$) (反证法)假设 $(a,n)=1$. 因 $[a]$ 是 $\mathbb{Z}_n$ 的零因子，故 $\exists [b]\in\mathbb{Z}_n$，$[b]\neq[0]$，使得 $[a][b]=[ab]=[0]$，即 $n\mid ab$. 因 $(a,n)=1$，从而 $n\mid b$，于是 $[b]=[0]$，矛盾. 所以 $(a,n)\neq 1$. (另一证法：若 $(a,n)=1$，由上面 1)($\Leftarrow$)的证明中知 $[u][a]=[1]$. 设 $[a][b]=[0]$，则 $[u][a][b]=[u][0]$，即 $[1][b]=[0]$，$[b]=[0]$，从而 $[a]$ 不是零因子，矛盾. 所以 $(a,n)\neq 1$. 还可利用第九章，三，1，3)，①知，$[a]$ 不是 $\mathbb{Z}_n$ 的可逆元，再由上面 1)($\Leftarrow$)，$(a,n)\neq 1$.)

注 ① 模 n 的剩余类环 $\mathbb{Z}_n$ 中可逆元的个数恰是欧拉(Euler)函数 $\phi(n)$，即小于 n 且与 n 互素的正整数的个数. 当 p 是素数时，$\mathbb{Z}_p$ 中可逆元恰有 $\phi(p)=p-1$ 个，从而 $\mathbb{Z}_p$ 中每个非零元都可逆. 因此 $\mathbb{Z}_n$ 的可逆元完全被刻划清楚了.

② $[a]$ 不是 $\mathbb{Z}_n$ 的可逆元 $\Leftrightarrow (a,n)\neq 1 \Leftrightarrow [a]$ 是 $\mathbb{Z}_n$ 的零因子.

例 找出 $\mathbb{Z}_{10}$ 的可逆元与零因子.

解 因 $(1,10)=(3,10)=(7,10)=(9,10)=1$，故 $\mathbb{Z}_{10}$ 有 $\phi(10)=4$ 个可逆元，且 $[1]$，$[3]$，$[7]$，$[9]$ 是可逆元，$[1]^{-1}=[1]$，$[3]^{-1}=[7]$，$[7]^{-1}=[3]$，$[9]^{-1}=[9]$. $\mathbb{Z}_{10}$ 中其余的 5 个非零元 $[2]$，$[4]$，$[5]$，$[6]$，$[8]$ 都是零因子.

12. 设 $\mathbb{Z}_n$ 是模 n 的剩余类环，$n\neq 1$，

证明：

$$n \text{ 是素数} \Leftrightarrow \mathbb{Z}_n \text{ 无零因子}.$$

证 ($\Leftarrow$) 若 n 不是素数，又 $n\neq 1$，则 n 是合数，从而 $\exists n_1,n_2\in\mathbb{Z}$，使得 $n=n_1n_2$，$1<n_i<n$，$i=1,2$. 于是 $n\nmid n_1$，$n\nmid n_2$，因此 $[n_1]\neq[0]$，$[n_2]\neq[0]$. 但 $[n_1][n_2]=[n_1n_2]=[n]$

$=[0]$. 所以 $\mathbb{Z}_n$ 有零因子，此与已知矛盾，从而 n 是素数.

（$\Rightarrow$）　$\forall [a],[b]\in\mathbb{Z}_n$，若 $[a][b]=[0]$，$[a]\neq[0]$，即 $[ab]=0$，从而 $n\mid ab$. 因 n 是素数，$n\nmid a$ 故 $n\mid b$，于是 $[b]=[0]$. 所以 $\mathbb{Z}_n$ 无零因子.（另一证法：因 n 是素数，又 $1\leqslant a<n$，故 $(a,n)=1$. 由上面题 11,2)（$\Rightarrow$），$[a]$ 不是零因子，所以 $\mathbb{Z}_n$ 无零因子.）

注　当 n 是合数时，$\mathbb{Z}_n$ 有零因子. 而且，$\mathbb{Z}_n$ 中的元除去零元 $[0]$ 以外，要么是可逆元，如果不是可逆元，就是零因子. 因 $\mathbb{Z}_n$ 中有 $\phi(n)$ 个可逆元，故 $\mathbb{Z}_n$ 中有 $n-1-\phi(n)$ 个零因子. 所以 $\mathbb{Z}_n$ 的零因子完全被刻划清楚了.

四、思考问题

1. 下列各集 R 对于数的加法与乘法是否作成环？

1)　$\{2a+1\mid a\in\mathbb{Z}\}$.

2)　$\{a\sqrt{3}\mid a\in\mathbb{Z}\}$.

3)　$\{bi\mid b\in\mathbb{R}\}$.

4)　R 是所有正整数的集.

5)　$\{a+b\sqrt{2}+c\sqrt{5}\mid a,b,c\in\mathbb{Z}\}$.

6)　$\left\{\frac{a}{b}\,\middle|\, a\in\mathbb{Z}, b=2q+1, q\in\mathbb{Z}\right\}$.

7)　$\left\{\frac{m}{2^n}\,\middle|\, m\in\mathbb{Z}, n\geqslant 0 \text{ 的整数}\right\}$.

2. 下面各集 R 对于规定的 $\oplus$ 与 $\odot$ 是否作成环？若 R 是环，则 R 是否有单位元？

1)　$R=\left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix}\,\middle|\, a,b,c,d\in\mathbb{R}, \begin{vmatrix} a & b\\ c & d\end{vmatrix}=0\right\}$. $\oplus$：矩阵加法，$\odot$：矩阵乘法.

2)　R 是实数集. $\oplus$：普通加法. $\odot$：$a\odot b=|a|b$.

3)　R 是整数集. $\oplus$：$a\oplus b=a-b-2$. $\odot$：普通乘法.

4)　R 对于 $+$ 与 $\cdot$ 作成一个有单位元 1 的环. $\oplus$：$a\oplus b=a+b-1$. $\odot$：$a\odot b=a+b-ab$.

3. 写出模 5 的剩余类环 $\mathbb{Z}_5$ 的加法表与乘法表.

4. 在模 12 的剩余类环 $\mathbb{Z}_{12}$ 中，求出下列各方程的解.

1)　$[4]x=[3]$.

2)　$[4]x=[4]$.

3)　$x^2-1=0$.

5. 在环 R 中，若 a 与 b 可换，即 $ab=ba$，证明：a 与 $-b$、与 $nb(n\in\mathbb{Z})$、与 b^{-1} 也都可换. 若 a 与 b、c 都可换，证明：a 与 $b+c$、与 bc 也都可换.

6. 在有单位元 1 的环 R 中，证明：

$$a \text{ 是 } R \text{ 的可逆元} \Leftrightarrow \exists\, b\in R, \text{使得 } aba=a, ba^2b=1.$$

7. 在有单位元 1 的环中，若 $a,b,ab-1$ 都可逆，证明：$a-b^{-1}$ 与 $(a-b^{-1})^{-1}-a^{-1}$ 也可

逆，且

$$[(a-b^{-1})^{-1}-a^{-1}]^{-1}=aba-a.$$

8. 设环 R 有单位元 $1,a,b\in R$. 若 $1-ab$ 在 R 中有逆元 x，证明：$1-ba$ 在 R 中也有逆元 $1+bxa$.

9. 求出环 $R=\{a+b\mathrm{i}\mid a,b\in\mathbb{Z}\}$ 的可逆元.

10. 在环中，若 $ab=ac$，$a\neq 0$ 且 a 不是左零因子，证明：$b=c$.

11. 设 a 是环 R 的非零元，$\exists\, b\in R$，$b\neq 0$，使得 $aba=0$. 证明：a 是左零因子或右零因子.

12. 首先给出下面的定义：设 $a\in$ 环 R. 若 $a^2=a$，则称 a 为 R 的幂等元. 若 $\exists$ 正整数 n，使得 $a^n=0$，则称 a 为 R 的幂零元. 证明：

1） 若 R 是有单位元 1 的无零因子环，则 R 的幂等元有且只有 0 与 1.

2） 若环 R 无零因子，则 R 的幂零元有且只有 0.

3） 若环 R 无零因子，且 $R\neq\{0\}$，则 e 是 R 的非零幂等元 $\Leftrightarrow$ e 是 R 的单位元.

4） 非零环 R 中的每个非零的幂零元都是零因子.

5） 设环 R 有单位元 1，x 是 R 的幂零元，则 $1-x$ 是 R 的可逆元，并求其逆元.

6） 若环 K 中的任意元都是幂零元，则称 K 为幂零元环. 交换环 R 中所有幂零元的集 S 作成一个幂零元环.

7） 在环 R 中，下列两条件等价：

① R 没有非零的幂零元；

② 如果 $a\in R$ 且 $a^2=0$，那么 $a=0$.

13. 设环 R 中任意元都是幂等元，即 $\forall\, x\in R$，$x^2=x$，则称 R 为布尔环. 证明：

1） $\forall\, x\in R$，$x+x=0$.

2） $\forall\, x,y\in R$，$xy=yx$.

14. 设代数系统 R 满足除加法交换律以外的环的定义中的所有条件，且 R 无零因子，证明：R 是一个环.

第十章　除环、域、无零因子环的特征

一、基本问题问答

1. 试判断下列各命题是否正确.

1）除环 R 的定义中的第一条："R 至少包含一个不等于零的元"可由第二条："R 有一个单位元"推出.

2）除环 R 中任意元 a 都在 R 中有逆元 a^{-1}.

3）除环和域中两个乘法消去律都成立.

4）设 $a,b\in$域 F，且 $2a=2b$，由域中消去律成立，有 $a=b$.

5）域 F 对于乘法来说作成一个群.

6）设 R 是一个环，则

$$R\text{ 是除环}\Leftrightarrow R^*=R-\{0\}\text{对于 }R\text{ 的乘法来说作成一个群.}$$

7）F 是域 $\Leftrightarrow F$ 是除环且 F 是整环.

8）整环是除环.

9）除环是整环.

答　1）不正确．因为只由第二条，R 可以是零环$\{0\}$.

2）不正确．因为除环 $R\neq\{0\}$，所以 R 中的零元 0 必无逆元(见第九章，一，10，2)).

3）正确．事实上，除环和域没有零因子，从而其中两个乘法消去律都成立.

4）不正确．例，$\mathbb{Z}_2=\{[0],[1]\}$是一个域，虽 $2[1]=2[0]$，但$[1]\neq[0]$.

5）不正确．因为域 $F\neq\{0\}$，而 $0\in F$，但零元 0 在 F 中必无逆元(见上面本题中的 2)).

6）正确．事实上，

（$\Rightarrow$）显然.

（$\Leftarrow$）已知 R 是环.

① 因 $R^*=R-\{0\}$是乘群，故 $R^*\neq\phi$，从而 R 至少包含一个不等于零的元.

② 因 $R^*=R-\{0\}$是乘群，故 R^* 有单位元 $1\in R$，显然 1 也是 R 的单位元.

③ 因 $R^*=R-\{0\}$是乘群，故 $\forall a\in R^*$，即 $\forall a\in R$，$a\neq0$，a 在 R^* 中有逆元，即 a 在 R 中有逆元.

综上，R 是除环.

注　设 R 是交换环，则

$$R\text{ 是域}\Leftrightarrow R^*=R-\{0\}\text{对于 }R\text{ 的乘法来说作成一个群.}$$

7）正确．事实上，

（$\Rightarrow$）因 F 是域，故 F 是交换除环，且 F 有单位元，无零因子，从而 F 也是整环.

($\Leftarrow$) 因 F 是除环,又是整环,故 F 中乘法适合交换律,从而 F 是域.

8) 不正确.例,整数环是整环,但不是除环.

9) 不正确.例,四元数除环是除环,但不是整环.

2. 设 $\mathbb{Z}_n$ 是模 n 的剩余类环.证明:

$$n\text{是素数} \Leftrightarrow \mathbb{Z}_n\text{是域}.$$

证一 ($\Rightarrow$) 利用"$\mathbb{Z}_n$ 是交换环,则

$$\mathbb{Z}_n\text{是域} \Leftrightarrow \mathbb{Z}_n^* = \mathbb{Z}_n - \{[0]\}\text{是乘群}"$$

可给出证明.

($\Leftarrow$) (反证法)若 n 不是素数,因 $\mathbb{Z}_n$ 是域,故 $\mathbb{Z}_n \neq \{[0]\}$,即 $n \neq 1$,从而 n 是合数.由第九章,三,12,$\mathbb{Z}_n$ 有零因子,于是 $\mathbb{Z}_n$ 不是域,此与已知矛盾.所以 n 是素数.

证二 ($\Rightarrow$) 下面直接利用域的定义来证明.已知 $\mathbb{Z}_n$ 是一个环.

1) 因 n 是素数,故 $n>1$,从而 $\exists [1](\neq [0]) \in \mathbb{Z}_n$.

2) $\mathbb{Z}_n$ 有单位元 $[1]$.

3) $\forall [a] \in \mathbb{Z}_n, [a] \neq [0]$,从而 $n \nmid a$.因 n 是素数,故 $(n,a)=1$.由第九章,三,11,1),$[a]$ 是 $\mathbb{Z}_n$ 的可逆元.

综上,$\mathbb{Z}_n$ 是一个除环.又 $\mathbb{Z}_n$ 的乘法可交换,于是 $\mathbb{Z}_n$ 是域.

($\Leftarrow$) 见证一.

证三 ($\Rightarrow$) 利用第十章,二,3来证明.因 n 是素数,故 $n>1$,即 $\mathbb{Z}_n$ 至少有两个元,且由第九章,三,12,$\mathbb{Z}_n$ 是无零因子的有限环.由第十章,二,3,$\mathbb{Z}_n$ 是除环.又 $\mathbb{Z}_n$ 的乘法可交换,所以 $\mathbb{Z}_n$ 是域.

($\Leftarrow$) 见证一.

注 对于任意一个素数 p,必存在含 p 个元的有限域.例如,$\mathbb{Z}_p$ 就是恰含素数 p 个元的有限域.

例 $\mathbb{Z}_{11}, \mathbb{Z}_{17}, \mathbb{Z}_{101}$ 都是域.$\mathbb{Z}_4, \mathbb{Z}_{51}, \mathbb{Z}_{471}$ 都不是域.

3. 环 R 的特征的定义是什么?

答 若 R 是无零因子环,$a \in R, a \neq 0$,则把 a 对于加法来说的阶叫做环 R 的特征.记为 $\mathrm{ch}\,R$.

也可如下表述:设 R 是无零因子环,则

$$\begin{array}{l} n\text{是}R\text{的特征} \\ \text{记为 }\mathrm{ch}\,R=n \end{array} \Leftrightarrow \exists\text{最小正整数 }n\text{,使得 }\forall a \in R, na=0,$$

$$\begin{array}{l} R\text{的特征是无限大} \\ \text{记为 }\mathrm{ch}\,R=\infty \end{array} \Leftrightarrow \overline{\exists}\text{正整数 }n\text{,使得 }\forall a \in R, na=0.$$

4. 在环 R 的特征的定义中,

1) 为什么要求 R 是无零因子环?

2) 为什么不考虑 R 中的零元 0 对于加法来说的阶?

3) 为什么不考虑 R 中的元对于乘法来说的阶?

答 1) 因为当 R 是无零因子环时,R 里所有不等于零的元对于加法来说的阶都是一

样的[①]．这样才能保证环 R 的特征是唯一确定的．而在有零因子环如 $\mathbb{Z}_4$ 中，[2]与[3]对于加法来说的阶却分别是 2 与 4.

2)　因为在 R 中有且只有零元对于加法来说的阶是 1，因此 R 中所有的元，当然包括零元对于加法来说的阶就肯定不相同，无法保证环 R 的特征的唯一性.

3)　因为定义元的阶时，该元必须是一个群中的元，但是环 $R(\neq\{0\})$ 对于乘法来说不能作成一个群（见本章，一，1，5）解答），所以就无从谈起环 R 中的元对于乘法来说的阶.

5. 试回答下列各问题.

1)　设 R 是无零因子环. 命题"$\forall$ 正整数 m，$\forall a\in R, a\neq 0$，有 $ma\neq 0$"在环 R 满足什么条件时才成立？

2)　无零因子环 R 的特征能是 1 吗？

3)　零环 $\{0\}$ 的特征是什么？

4)　数环 $(\neq\{0\})$ 与数域的特征是什么？

5)　实系数多项式环 $\mathbf{R}[x]$ 的特征是什么？

6)　设 p 是素数，$\mathbb{Z}_p$ 的特征是什么？

7)　有限整环 $R(\neq\{0\})$ 的特征是什么？

8)　四元数除环的特征是什么？

9)　设 R 是布尔环，即 $\forall x\in R, x^2=x$（见第九章，四，13）. 又设 R 无零因子且不等于 $\{0\}$. $\mathrm{ch}\,R=?$

10)　设 R 是 2^n（n 是正整数）阶整环，问 $\mathrm{ch}\,R=?$

11)　若无零因子环 R 的特征是 p，则 R 至少有多少个元？

答　1)　设 R 是无零因子环，则

$$\mathrm{ch}\,R=\infty \Leftrightarrow \forall \text{正整数}\, m,\ \forall a\in R,\ a\neq 0, \text{有}\ ma\neq 0.$$

2)　无零因子环 R 的特征不能是 1. 因为 R 的特征是 R 的非零元对于加法来说的阶，而这些非零元的阶绝不是 1，所以 $\mathrm{ch}\,R\neq 1$.

3)　零环 $\{0\}$ 无特征．此由特征定义可知.

4)　数环 $(\neq\{0\})$ 与数域的特征是 ∞. 因为数环与数域是无零因子环，其中任意非零数 a，对于任意正整数 m，有 $ma\neq 0$.

5)　实系数多项式环 $\mathbf{R}[x]$ 的特征是 ∞. 因 $\mathbf{R}[x]$ 无零因子．1 是 $\mathbf{R}[x]$ 的单位元，若 $m1=0$，则 $m=0$，从而 1 对于加法来说的阶是 ∞，所以 $\mathrm{ch}\,\mathbf{R}[x]=\infty$.

注　在有单位元 1 的无零因子环 R 中，由 1 对于加法来说的阶即可知 $\mathrm{ch}\,R$. 这样判断 $\mathrm{ch}\,R$ 比较方便.

6)　有限域 $\mathbb{Z}_p$ 的特征是 p. 因为 $\mathbb{Z}_p$ 无零因子，其单位元[1]对于加法来说的阶是 p，所以 $\mathrm{ch}\,\mathbb{Z}_p=p$.

7)　有限整环 R 是一个无零因子环，且 R 是一个有限加群．因此，由第四章，二，7 知，R 中所有不等于零的元对于加法来说的阶都是一个相同的有限整数，所以 R 的特征是一个素数.

注　①　有限除环和有限域的特征都是素数.

① 张禾瑞．近世代数基础．北京：高等教育出版社，1978. 95. 定理 1.

② 若整环 R 的特征是∞，则 R 有无限多个元.

8) 四元数除环 R 的特征是∞. 因 R 无零因子，$(1,0)$是 R 的单位元，$\forall$ 正整数 m，$m(1,0)=(m,0)\neq(0,0)$，从而$(1,0)$对于加法来说的阶等于∞，所以 $\mathrm{ch}\,R=\infty$.

9) 由第九章，四，13 知，$\forall x\in R$，$2x=x+x=0$. 又 R 无零因子，且 $R\neq\{0\}$，从而 R 的非零元对于加法来说的阶等于 2，所以 $\mathrm{ch}\,R=2$.

10) 因 R 是非零有限整环，故 $\mathrm{ch}\,R$ 是素数(见本题 7)). 由特征定义可得 $\mathrm{ch}\,R \mid |R|=2^n$. 所以 $\mathrm{ch}\,R=2$.

11) 已知 $\mathrm{ch}\,R=p$，由特征定义，$\exists a\in R, a\neq 0$，a 对于加法来说的阶等于 p. 由第四章，一，7 知，R 中至少有 p 个不同的元：

$$0a=0,\ a,\ 2a,\ \cdots,\ (p-1)a.$$

二、典型问题分析

1. $F=\{$所有复数 $a+b\mathrm{i}$(a,b 是有理数)$\}$. 证明：F 对于普通加法和乘法来说是一个域.

证 用证明第九章，二，6 的同样方法可证明 F 是一个整环．又

1) F 有 $1\neq 0$.

2) $\forall a+b\mathrm{i}\in F$，$a+b\mathrm{i}\neq 0$，即 a,b 不全为 0，从而 $a^2+b^2\neq 0$. 设 $\alpha(a+b\mathrm{i})=(a+b\mathrm{i})\alpha=1$，这里 1 是 F 的单位元．则

$$\alpha=\frac{1}{a+b\mathrm{i}}=\frac{a}{a^2+b^2}+\frac{-b}{a^2+b^2}\mathrm{i}\in F$$

是 $a+b\mathrm{i}$ 的逆元．所以 F 是一个域.

注 记 $F=\mathbf{Q}(\mathrm{i})$，它是包含有理数域 $\mathbf{Q}$ 与 i 的最小数域.

2. $F=\{$所有实数 $a+b\sqrt{3}$，(a,b 是有理数)$\}$. 证明：F 对于普通加法和乘法来说是一个域.

证 仿上面题 1，可证 F 是一个整环．且 F 有 $1\neq 0$. $\forall a+b\sqrt{3}\in F$，$a+b\sqrt{3}\neq 0$，即 a,b 中至少有一个不等于零，则 $a^2-3b^2\neq 0$. 不然，若 $a^2-3b^2=0$，即 $a^2=3b^2$，$a=\pm\sqrt{3}b$. 因 a 是有理数，$\sqrt{3}$是无理数，故 $b=0$，从而 $a=0$，此与 a,b 不全为 0 矛盾．所以 $a^2-3b^2\neq 0$. 容易验证

$$\frac{1}{a+b\sqrt{3}}=\frac{a}{a^2-3b^2}+\frac{-b}{a^2-3b^2}\sqrt{3}\in F$$

是 $a+b\sqrt{3}$的逆元．于是 F 是一个域.

注 记 $F=\mathbf{Q}(\sqrt{3})$，它是包含有理数域 $\mathbf{Q}$ 与$\sqrt{3}$的最小数域.

3. 证明：一个至少有两个元而且没有零因子的有限环是一个除环.

证 设 R 是一个没有零因子的有限非零环，要证 R 是一个除环，只需证明 $R^*=R-\{0\}$是一个乘群．因 R 是非零环，故 R 至少包含一个不等于零的元，即 $R^*\neq\varnothing$.

Ⅰ. $\forall a,b\in R^*$，$a\neq 0, b\neq 0$，因 R 无零因子，故 $ab\neq 0$，从而 $\exists\,|\,ab\in R^*$，于是 R^* 对乘法封闭.

Ⅱ. R^* 中乘法适合结合律.

Ⅲ′. 环 R 中消去律成立[①]，从而 R^* 中消去律成立，即：$\forall a,b,c\in R$，若 $ab=ac$，则 $b=c$；若 $ba=ca$，则 $b=c$.

因 R^* 是有限集，故由有限群的另一定义[②]，R^* 是乘群．由第十章，1,6）知 R 是一个除环.

注　1）　设 R 是有限环，则

$$R\text{ 至少含两个元且 }R\text{ 无零因子}\Leftrightarrow R\text{ 是除环}.$$

2）　1）的逆否命题：设 R 是有限环且 $R\neq\{0\}$，则

$$R\text{ 不是除环}\Leftrightarrow R\text{ 有零因子}.$$

3）　设 R 是有限交换环，则

$$R\text{ 至少含两个元且 }R\text{ 无零因子}\Leftrightarrow R\text{ 是域}.$$

对于有限环来说判断是否为域用此条件较定义简便（见第十章，一，2）.

4）　设 R 是有限非零环，则

$$R\text{ 是整环}\Leftrightarrow R\text{ 是域}.$$

证一　（$\Rightarrow$）　由该命题即知 R 是域.

（$\Leftarrow$）　显然.

证二　（$\Rightarrow$）　首先证明：若 R 是有单位元 1 的含有限个元的交换环，则 R 的元，除零元外不是可逆元就是零因子（参看第九章，三，1,4））.

事实上，当 $R=\{0\}$ 时，命题显然成立．当 $R\neq\{0\}$ 时，设 R 含 $n(>1)$ 个元．若 $a(\in R)$ 不是可逆元，$a\neq 0$，则 $\bar{\exists}\, x\in R$，使得 $ax=1$. 作集 $P=\left\{ar\,\middle|\,r\in R\right\}$，于是 $P\subset R$ 且 $1\bar{\in} P$，即 P 是 R 的真子集，P 含元的个数小于 n. 因 R 含 n 个元，故形如 $ar(r\in R)$ 的元可写出 n 个，因此，$\exists\, r_1,r_2\in R,r_1\neq r_2$，使得 $ar_1=ar_2$，即 $a(r_1-r_2)=0$. 因 $r_1-r_2\neq 0,a\neq 0$，故 a 是 R 的左零因子. 同理可证 a 也是 R 的右零因子，即 a 是零因子.

由题设，R 是有限非零整环，从而 R 的元除零元外不是可逆元就是零因子．今 R 无零因子，因此 R 的每个非零元都是可逆元，由定义 R 是域.

（$\Leftarrow$）　显然.

无限整环未必是域，如整数环 $\mathbf{Z}$. 但非零有限整环必为域.

4. 设 $R=\{$所有复数对$(\alpha,\beta)\}$. 这里

$$(\alpha_1,\beta_1)=(\alpha_2,\beta_2)\text{，当而且只当 }\alpha_1=\alpha_2,\beta_1=\beta_2\text{ 的时候}.$$

R 的加法和乘法是

$$(\alpha_1,\beta_1)+(\alpha_2,\beta_2)=(\alpha_1+\alpha_2,\beta_1+\beta_2),$$
$$(\alpha_1,\beta_1)(\alpha_2,\beta_2)=(\alpha_1\alpha_2-\beta_1\bar{\beta}_2,\alpha_1\beta_2+\beta_1\bar{\alpha}_2).$$

这里 $\bar{\alpha}$ 表示的是 α 的共轭数：

$$\alpha=\alpha_1+\alpha_2\mathrm{i},\ \bar{\alpha}=\alpha_1-\alpha_2\mathrm{i}(\alpha_1,\alpha_2\text{ 是实数}).$$

则 R 是一个除环．这个环叫做四元数除环．

详细证明：R 的乘法适合结合律.

---

① 张禾瑞．近世代数基础．北京：高等教育出版社，1978. 88. 定理

② 同上．39.

证 $\forall(\alpha_1,\beta_1),(\alpha_2,\beta_2),(\alpha_3,\beta_3)\in R$,

$$[(\alpha_1,\beta_1)(\alpha_2,\beta_2)](\alpha_3,\beta_3)=(\alpha_1\alpha_2-\beta_1\bar{\beta}_2,\alpha_1\beta_2+\beta_1\bar{\alpha}_2)(\alpha_3,\beta_3)$$

$$=\Big((\alpha_1\alpha_2-\beta_1\bar{\beta}_2)\alpha_3-(\alpha_1\beta_2+\beta_1\bar{\alpha}_2)\bar{\beta}_3,(\alpha_1\alpha_2-\beta_1\bar{\beta}_2)\beta_3+(\alpha_1\beta_2+\beta_1\bar{\alpha}_2)\bar{\alpha}_3\Big).$$

又

$$(\alpha_1,\beta_1)[(\alpha_2,\beta_2)(\alpha_3,\beta_3)]=(\alpha_1,\beta_1)(\alpha_2\alpha_3-\beta_2\bar{\beta}_3,\alpha_2\beta_3+\beta_2\bar{\alpha}_3)$$

$$=\Big(\alpha_1(\alpha_2\alpha_3-\beta_2\bar{\beta}_3)-\beta_1\overline{(\alpha_2\beta_3+\beta_2\bar{\alpha}_3)},\alpha_1(\alpha_2\beta_3+\beta_2\bar{\alpha}_3)+\beta_1\overline{(\alpha_2\alpha_3-\beta_2\bar{\beta}_3)}\Big)$$

$$=\Big(\alpha_1\alpha_2\alpha_3-\alpha_1\beta_2\bar{\beta}_3-\beta_1\Big(\overline{\alpha_2\beta_3}+\overline{\beta_2\bar{\alpha}_3}\Big),\alpha_1\alpha_2\alpha_3+\alpha_1\beta_2\bar{\alpha}_3+\beta_1\overline{(\alpha_2\alpha_3}-\overline{\beta_2\bar{\beta}_3)}\Big)$$

$$=\Big(\alpha_1\alpha_2\alpha_3-\alpha_1\beta_2\bar{\beta}_3-\beta_1\bar{\alpha}_2\bar{\beta}_3-\beta_1\bar{\beta}_2\alpha_3,\alpha_1\alpha_2\beta_3+\alpha_1\beta_2\bar{\alpha}_3+\beta_1\bar{\alpha}_2\bar{\alpha}_3-\beta_1\bar{\beta}_2\beta_3\Big)$$

$$=\Big((\alpha_1\alpha_2-\beta_1\bar{\beta}_2)\alpha_3-(\alpha_1\beta_2+\beta_1\bar{\alpha}_2)\bar{\beta}_3,(\alpha_1\alpha_2-\beta_1\bar{\beta}_2)\beta_3+(\alpha_1\beta_2+\beta_1\bar{\alpha}_2)\bar{\alpha}_3\Big).$$

所以

$$[(\alpha_1,\beta_1)(\alpha_2,\beta_2)](\alpha_3,\beta_3)=(\alpha_1,\beta_1)[(\alpha_2,\beta_2)(\alpha_3,\beta_3)].$$

5. 验证,四元数除环的任意元$(a+bi,c+di)$,这里a,b,c,d是实数,可以写成

$$(a,0)+(b,0)(i,0)+(c,0)(0,1)+(d,0)(0,i)$$

的形式.

证

$$(a+bi,c+di)=(a,c)+(bi,di)$$
$$=(a,0)+(bi,0)+(0,c)+(0,di)$$
$$=(a,0)(1,0)+(b,0)(i,0)+(c,0)(0,1)+(d,0)(0,i).$$

6. 假定F是一个有四个元的域.

证明:

1) F的特征是2;

2) F的不等于零或1的两个元都适合方程$x^2=x+1$.

证一 1) 因F是有限加群,故由第四章,二,7知,F的每一个元的阶都有限. 因F是无零因子环,故F的非零元的阶都相同. 因此$\forall s\in F,s\neq0$,可设s的阶=正整数n,则$n\mid 4$,且n是素数[①],于是$n=2$,所以ch $F=2$.

2) 设$F=\{0,1,a,b\}$. 已知ch $F=2$,从而$1+1=0,a+a=0,b+b=0$. 因0是F的零元,故$0+0=0,0+1=1,0+a=a,0+b=b$. 由F的加法适合消去律,$1+a\neq a,1+a\neq1$. 又$1+a\neq0$(不然,若$1+a=0$,则$a=-1=1$,矛盾),所以$1+a=b$. 同理$1+b=a,a+b=1$. 又由F的加法适合交换律,从而有加法表:

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

① 张禾瑞. 近世代数基础. 北京:高等教育出版社,1978. 96. 定理2.

因 F 是域，故 $F^*=F-\{0\}=\{1,a,b\}$ 是一个 3 阶乘群．由 F^* 的乘法适合消去律，$ab\neq a$，$ab\neq b$，所以 $ab=1$. 又 $a^2\neq a$，$a^2\neq 1$（不然，若 $a^2=1$，又 $ab=1$，于是 $a^2=ab$，即 $a=b$，矛盾），所以 $a^2=b$. 同理 $b^2=a$. 由 F 的乘法适合交换律，$ba=1$. 于是有乘法表：

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

显见，$a^2=b=a+1$，$b^2=a=b+1$.

证二 1) 若 ch $F\neq 2$，即 F 的不等于零的元的阶不等于 2，从而把 F 看成加群．由第七章，二，11，F 与模 4 的剩余类加群 $\mathbf{Z}_4$ 同构，于是在 F 中必有 4 阶元．由 F 是无零因子环，F 中 3 个非零元的阶都是 4，此与第四章，二，5 矛盾．所以 ch $F=2$.

2) 因 F 是有 4 个元的域，故由第七章，二，6，$F^*=F-\{0\}$ 是一个 3 阶循环乘群，即 $F^*=(a)=\{1,a,a^2\}$，其中 $a^3=1$，从而 $F=\{0,1,a,a^2\}$. 因 ch $F=2$，故 $a+1\neq 0$. 因 F 的加法适合消去律，故 $a+1\neq 1$，$a+1\neq a$，从而 $a+1=a^2$. 又由 ch $F=2$，$a^2+1=a^2+(-1)=a=a^3a=a^4=(a^2)^2$. 所以 F 的不等于零或 1 的两个元都适合方程 $x^2=x+1$.

证三 1) 因域 F 中共有 3 个非零元，故必有一个非零元 a 的负元是本身，即 $a=-a$，$2a=0$，a 的阶$=2$. 又 F 是无零因子环，所以 ch $F=2$.

2) 因 $F=\{0,1,a_1,a_2\}$ 是域，故 $F^*=F-\{0\}=\{1,a_1,a_2\}$ 是乘群，且 F^* 的阶是素数 3. 又 a_i 的阶不等于 1，从而 a_1 与 a_2 的阶都是 3，即 $a_i^3-1=0$，于是 $(a_i-1)(a_i^2+a_i+1)=0$，$i=1,2$. 因 $a_i-1\neq 0$，又域 F 无零因子，故 $a_i^2+a_i+1=0$，即 $a_i^2=-a_i+(-1)$. 因 ch $F=2$，故 F 的非零元的阶都是 2，即 $-a_i=a_i$，$-1=1$，所以 $a_i^2=a_i+1$ ，$i=1,2$.

证四 1) 假设 ch $F=3$，则 F 中 3 个非零元的阶都是 3，此与第四章，二，5 矛盾．所以 ch $F\neq 3$. 又 ch F 是 $\leqslant 4$ 的一个素数，从而 ch $F=2$.

2) 见证一.

证五 1) 因 F 是 $4=2^2$ 阶整环，故由第十章，一，5，10)，ch $F=2$.

2) 见证一.

注 因 $F^*=F-\{0\}$ 是 3 阶循环乘群，从同构观点看，3 阶循环乘群只有 1 个，故四元域也只有 1 个.

7. 假定[a]是模 n 的一个剩余类．证明：若 a 同 n 互素，那么所有[a]的数都同 n 互素（这时我们说[a]同 n 互素）.

证一 $\forall x\in[a]$，设 $(x,n)=d$，则 $\exists x_1,n_1\in\mathbf{Z}$，使得 $x=dx_1$，$n=dn_1$. 因 $x\in[a]$，故 $n\mid a-x$，从而 $\exists q\in\mathbf{Z}$，使得 $a-x=nq$，于是

$$a=x+nq=dx_1+dn_1q=d(x_1+n_1q),$$

其中 $x_1+n_1q\in\mathbf{Z}$. 因此 $d\mid a$，又 $d\mid n$，有 $d\mid(a,n)=1$. 所以 $d=(x,n)=1$.

证二 $\forall x\in[a]$，有 $n\mid a-x$，从而 $\exists q\in\mathbf{Z}$，使得 $a-x=qn$，即 $a=x+qn$. 又因 $(a,n)=1$，故 $\exists u,v\in\mathbf{Z}$，使得 $ua+vn=1$，即 $u(x+qn)+vn=1$，$ux+(uq+v)n=1$，其中 $u,uq+v\in$

$\mathbb{Z}$. 所以$(x,n)=1$.

8. 证明:所有同 n 互素的模 n 的剩余类对于剩余类的乘法来说作成一个群(同 n 互素的剩余类的个数一般用符号$\phi(n)$来表示,并且把它叫做尤拉ϕ函数).

证一 设 $G=\left\{[a]\,\middle|\,[a]\text{是模 } n \text{ 的剩余类},[a]\text{同 } n \text{ 互素}\right\}$,$n>1$. 今证 G 是群. 因$(1,n)=1$,故$[1]\in G$,从而 $G\neq\varnothing$.

1) $\forall [a],[b]\in G,[a][b]=[ab]$. 由$(a,n)=(b,n)=1$,有 $av+nu=1,bv'+nu'=1$,从而$(av+nu)(bv'+nu')=1$,

即

$$ab(vv')+n(buv'+avu'+nuu')=1.$$

所以$(ab,n)=1$.(另一证法:若$(ab,n)\neq1$,则有素数 p,使 $p\mid n,p\mid ab$,由 p 是素数,$p\mid a$ 或 $p\mid b$. 从而 p 是 a,n 的公因数或 p 是 b,n 的公因数. 此与$(a,n)=(b,n)=1$ 矛盾.)于是$[ab]\in G$.

若$[a']=[a],[b']=[b]$,则$[a'][b']=[a'b']\in G$. 下面证明$[a'b']=[ab]$. 事实上,由$[a']=[a],[b']=[b]$,有 $n\mid a'-a,n\mid b'-b$,从而 $n\mid a'(b'-b)+b(a'-a)=a'b'-ab$. 所以$[a'b']=[ab]$. 即$\exists\,|\,[ab]\in G$,使得$[a][b]=[ab]$.

2) 乘法适合结合律.

3) $\forall [a],[x],[x']\in G$,若$[a][x]=[a][x']$,则$[ax]=[ax']$,从而 $n\mid ax-ax'=a(x-x')$. 但$(n,a)=1$,于是 $n\mid x-x'$,即$[x]=[x']$. 所以左消去律成立. 同理可证右消去律成立.

综上,又 G 是有限集,因此 G 作成一个群.

证二 由证一,已证 $G\neq\varnothing$,G 对乘法封闭,结合律成立. 再证 G 有单位元,且每个元有逆元.

1) 因$(1,n)=1$,故$[1]\in G$,$[1]$是 G 的单位元.

2) $\forall [a]\in G,(a,n)=1$,从而$\exists u,v\in\mathbb{Z}$,使得 $ua+vn=1$,且$(u,n)=1$. 于是$[u][a]+[v][n]=[1]$,由$[n]=[0]$,有$[u][a]=[1]$. 又$[a][u]=[1]$,因此,$[a]$有逆元$[a]^{-1}=[a]$(见第九章,三,11,1)). 因$(u,n)=1$,故$[a]^{-1}=[u]\in G$.

综上,由群的定义知 G 是一个群.

注 见后面第十四章,四,7.

9. 证明:若是$(a,n)=1$,那么 $a^{\phi(n)}\equiv1(n)$[费马定理].

证 由上面 8 题知

$$G=\{[a]\mid[a]\text{是模 } n \text{ 的剩余类},[a]\text{同 } n \text{ 互素}\}$$

$(n>1)$是一个群. 已知$(a,n)=1$,从而$[a]\in G$. 且 $|[a]|\,\big|\,|G|=\phi(n)$,由第四章,一,6,$[a]^{\phi(n)}=[1]$. 又

$$[a]^{\phi(n)}=\overbrace{[a][a]\cdots[a]}^{\phi(n)\text{个}}=[\overbrace{a\,a\,\cdots\,a}^{\phi(n)\text{个}}]=[a^{\phi(n)}],$$

于是$[a^{\phi(n)}]=[1]$,即 $n\mid a^{\phi(n)}-1$. 所以 $a^{\phi(n)}\equiv1(n)$.

注 1) 设 p 是素数，a 是任一正整数，若 $(a,p)=1$，则 $a^{p-1}\equiv 1(p)$，即 $p\mid a^{p-1}-1$.

证 由该命题，有 $a^{\phi(p)}\equiv 1(p)$. 因 p 是素数，故 $\phi(p)=p-1$. 所以 $a^{p-1}\equiv 1(p)$.

2) 设 p 是素数，a 是任一正整数，则 $a^p\equiv a(p)$.

证 ① 若 $(a,p)=1$，则由注 1)，$p\mid a^{p-1}-1$. 显然 $p\mid a(a^{p-1}-1)=a^p-a$，即 $a^p\equiv a(p)$.

② 若 $(a,p)\neq 1$，因 p 是素数，故 $p\mid a$. 显然 $p\mid a^p-a$，即 $a^p\equiv a(p)$.

三、讲与练

1. 试判断以下各集 R 对于规定的＋、· 来说是否作成环，是否作成域.

1) $R=\left\{\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix} \middle| a\in\text{域 } F\right\}$. ＋：矩阵加法，·：矩阵乘法.（矩阵中除主对角线外的元素都是 0.）

2) $R=\left\{\begin{pmatrix} a & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{pmatrix} \middle| a\in\text{域 } F\right\}$. ＋：矩阵加法，·：矩阵乘法.（矩阵中除主对角线外的元素都是 0.）

3) $R=\left\{\begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{pmatrix} \middle| a_i\in\text{域 } F\right\}$，$n>1$. ＋：矩阵加法，·：矩阵乘法.（矩阵中除主对角线外的元素都是 0.）

4) $R=M_n(F)$，其中 F 是域，$n>1$. ＋：矩阵加法，·：矩阵乘法.

5) $R=\mathbf{R}[x]$. ＋：多项式加法，·：多项式乘法.

6) $R=\{0,1\}$.

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

7) $R=\{a,b,c\}$.

+	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

·	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

8) $R=\{a,b,c\}$.

+	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

·	a	b	c
a	a	a	a
b	a	b	c
c	a	c	c

解 1) R 是环也是域.

2) R 是环也是域.

3) R 是环但不是域．因 $\exists A=\begin{pmatrix}1 & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0\end{pmatrix}(\neq 0)\in R$，而 A 在 R 中无逆元.

4) R 是环但不是域．见第九章，三，7.

5) R 是环但不是域．因为次数大于零的多项式都不是可逆元.

6) R 是环且是域.

7) R 是环且是域.

8) R 不是环．因为 $c(b+c)=ca=a, cb+cc=c+c=b$，所以 $c(b+c)\neq cb+cc$.

2. 集 $R=\{(a_1,a_2)\mid a_1,a_2\in\mathbf{Q}\}$ 对于

$$(a_1,a_2)=(b_1,b_2)\Leftrightarrow a_1=b_1, \text{且 } a_2=b_2,$$
$$(a_1,a_2)+(b_1,b_2)=(a_1+b_1,a_2+b_2),$$
$$(a_1,a_2)(b_1,b_2)=(a_1b_1,a_2b_2)$$

来说能作成一个环吗？能作成一个域吗？

解 按环的定义逐条验证可知 R 作成一个环．(0,0)是 R 的零元．$\forall (a_1,a_2)\in R$，有负元 $(-a_1,-a_2)\in R$，且 R 有单位元(1,1)．当 $a_1\neq 0$ 且 $a_2\neq 0$ 时，$(a_1,a_2)(\in R)$ 有逆元 $\left(\frac{1}{a},\frac{1}{b}\right)\in R$. R 是交换环.

R 不能作成一个域．因为 R 有零因子，例，$(a,0)$，$(0,b)$（其中 $a\neq 0$ 且 $b\neq 0$）都是 R 的零因子.

注 1) 该命题可推广为如下命题：设 R_1 与 R_2 是两个环，则集 $R=\{(a_1,a_2)\mid a_1\in R_1,a_2\in R_2\}$ 对于

$$(a_1,a_2)=(b_1,b_2)\Leftrightarrow a_1=b_1 \text{ 且 } a_2=b_2,$$
$$(a_1,a_2)+(b_1,b_2)=(a_1+b_1,a_2+b_2),$$
$$(a_1,a_2)(b_1,b_2)=(a_1b_1,a_2b_2)$$

来说作成一个环．设 0_{R_1} 和 0_{R_2} 分别是 R_1 和 R_2 的零元，则 $0=(0_{R_1},0_{R_2})$ 是 R 的零元．$\forall (a_1,a_2)\in R$，有负元 $(-a_1,-a_2)\in R$．当 R_1 和 R_2 分别有单位元 1_{R_1} 和 1_{R_2} 时，R 有单位元 $(1_{R_1},1_{R_2})$．这时，(a_1,a_2) 是 R 的可逆元 $\Leftrightarrow a_1$ 和 a_2 分别是 R_1 和 R_2 的可逆元．再者，R 是交换环 $\Leftrightarrow R_1$ 和 R_2 都是交换环．但当 R_1 和 R_2 都无零因子时，R 未必无零因子.

2) 还可作如下推广：设 $R_1,R_2,\cdots,R_n$ 是 n 个环，则集 $R=\{(a_1,a_2,\cdots,a_n)\mid a_i\in R_i\}$ 对于

$$(a_1,a_2,\cdots,a_n)=(b_1,b_2,\cdots,b_n)\Leftrightarrow a_i=b_i, i=1,2,\cdots,n,$$
$$(a_1,a_2,\cdots,a_n)+(b_1,b_2,\cdots,b_n)=(a_1+b_1,a_2+b_2,\cdots,a_n+b_n),$$
$$(a_1,a_2,\cdots,a_n)(b_1,b_2,\cdots,b_n)=(a_1b_1,a_2b_2,\cdots,a_nb_n)$$

来说作成一个环.

3) 在该题中，将乘法定义改为

$$(a_1,a_2)(b_1,b_2)=(a_1b_1,a_2b_2),$$

则 R 仍能作成一个环．此时 R 不是交换环.

4)　设 $R=\{(a_1,a_2)\mid a_1,a_2\in\{奇,偶\}\}$.

+	奇	偶
奇	偶	奇
偶	奇	偶

·	奇	偶
奇	奇	偶
偶	偶	偶

是集{奇,偶}的两个代数运算,在 R 中规定

$$(a_1,a_2)=(b_1,b_2)\Leftrightarrow a_1=b_1 \text{ 且 } a_2=b_2,$$
$$(a_1,a_2)\oplus(b_1,b_2)=(a_1+b_1,a_2+b_2),$$
$$(a_1,a_2)\odot(b_1,b_2)=(a_1b_1,a_2b_2),$$

则 R 作成一个环．(偶,偶)是 R 的零元．$\forall(a_1,a_2)(\in R)$的负元就是其自身.

5)　$R=\{(a_1,a_2)\mid a_1,a_2\in\mathbf{R}\}$对于

$$(a_1,a_2)=(b_1,b_2)\Leftrightarrow a_1=b_1 \text{ 且 } a_2=b_2,$$
$$(a_1,a_2)+(b_1,b_2)=(a_1+b_1,a_2+b_2),$$
$$(a_1,a_2)(b_1,b_2)=(a_1b_1-a_2b_2,a_1b_2+a_2b_1)$$

来说作成一个域．(0,0)是 R 的零元．$\forall(a_1,a_2)\in R$,有负元$(-a_1,-a_2)\in R$.(1,0)是 R 的单位元．$\forall(a_1,a_2)(\neq(0,0)$,即 $a_1\neq0$ 或 $a_2\neq0)\in R$,有逆元$\left(\frac{a_1}{a_1^2+a_2^2},\frac{-a_2}{a_1^2+a_2^2}\right)\in R$. 实际上该 R 与复数域同构.

6)　在注 5)中,将乘法定义改为

$$(a_1,a_2)(b_1,b_2)=(a_1b_1-a_2b_2,-a_1b_2-a_2b_1),$$

R 不是一个环．因为乘法结合律不成立．取$(1,1),(0,1),(1,0)\in R$,有$[(1,1)(0,1)](1,0)=(-1,-1)(1,0)=(-1,1)$,但$(1,1)[(0,1)(1,0)]=(1,1)(0,-1)=(1,1)$.

3. 设环 $R\neq\{0\}$,证明:

$$R \text{ 是除环} \Leftrightarrow \forall a(\neq0),b\in R,\text{方程 } ax=b(\text{或 } ya=b)\text{在 } R \text{ 中有解}.$$

证　($\Rightarrow$)　因 R 是除环,故 $R^*=R-\{0\}$是乘群,从而$\forall a,b\in R,a\neq0$,当 $b\neq0$ 时,即 $a,b\in R^*$,方程 $ax=b$ 在 R^* 中有解,当然也在 R 中有解;当 $b=0$ 时,方程 $ax=0$ 有解 0 且 $0\in R$.

($\Leftarrow$)　$\forall a,b\in R^*$,由已知,方程 $ax=b$ 有解 $c\in R$,方程 $bx=c$ 有解 $d\in R$,即 $abd=ac=b$. 因 $b\neq0$,故 $ab\neq0$,从而 $ab\in R^*$,至此说明 R^* 对乘法封闭．又因 $a\neq0,b\neq0$,有 $ab\neq0$,故说明 R 无零因子,消去律成立.

下面再证明 R^* 有单位元．由 $R\neq\{0\}$,$\exists a(\neq0)\in R$,方程 $ax=a$ 有解 e 且 $e\in R^*$,即 $ae=a$. 两边右乘 e,$ae^2=ae$,因 $a\neq0$,故由消去律 $e^2=e$,即 e 是无零因子环的非零幂等元．由第九章,四,12,3),e 是 R 的,当然也是 R^* 的单位元.

最后,$\forall a\in R^*$,方程 $ax=e$ 在 R^* 中有解 a',即 $aa'=e$. 从而 a 有右逆元 $a'\in R^*$.

显然 R^* 中乘法适合结合律,且 $R^*\neq\varnothing$.

综上,R^* 是乘群．所以 R 是除环.

注　该命题给出了域的一个判别条件:设 F 是含非零元的交换环,则

$$F \text{ 是域} \Leftrightarrow \forall a(\neq0),b\in F,\text{方程 } ax=b(\text{或 } ya=b)\text{在 } F \text{ 中有解}.$$

4. 在一个特征是素数 p 的无零因子的交换环 R 里，证明：

1) $(a-b)^p=a^p-b^p$.

2) 对于任意非负整数 n，有 $(a\pm b)^{p^n}=a^{p^n}\pm b^{p^n}$.

3) 对每个整数 $n\geqslant 0$，

$$(a_1\pm a_2\pm\cdots\pm a_m)^{p^n}=a_1^{p^n}\pm a_2^{p^n}\pm\cdots\pm a_m^{p^n}.$$

4) 当 R 有单位元 1 时，$(n1)^p=n1$.

5) $(a-b)^{p-1}=a^{p-1}+a^{p-2}b+\cdots+ab^{p-2}+b^{p-1}$.

证 1) 我们有

$$(a-b)^p=(a+(-b))^p=a^p+(-b)^{p}\text{①}.$$

① 当 p 是奇素数时，

$$(a-b)^p=a^p+(-b)^p=a^p+(-b)^p=a^p-b^p.$$

② 当 p 是偶素数时，即 $p=2$. 因 $\operatorname{ch}R=2$，故 $2b^p=0$，从而 $b^p=-b^p$. 于是

$$(a-b)^p=a^p+(-b)^p=a^p+b^p=a^p+(-b^p)=a^p-b^p.$$

(还可如下证明：设 $a-b=x$，即 $a=x+b$，则 $a^p=(x+b)^p=x^p+b^p=(a-b)^p+b^p$. 所以 $(a-b)^p=a^p-b^p$.)

2) 对 n 作数学归纳法.

当 $n=0,1$ 时，命题显然成立.

假定 $n=k$ 时命题成立. 今看 $n=k+1$ 时，

$$(a\pm b)^{p^{k+1}}=\left((a\pm b)^{p^k}\right)^p=\left(a^{p^k}\pm b^{p^k}\right)^p=a^{p^{k+1}}\pm b^{p^{k+1}},$$

即 $n=k+1$ 时，命题也成立. 所以由归纳原理，命题成立.

3) 对 m 作数学归纳法.

当 $m=1$ 时，命题显然成立.

假定 $m=k$ 时命题成立. 今证 $m=k+1$ 时，命题也成立.

$$(a_1\pm a_2\pm\cdots\pm a_{k+1})^{p^n}=\left[(a_1\pm a_2\pm\cdots\pm a_k)\pm a_{k+1}\right]^{p^n}$$

$$=(a_1\pm a_2\pm\cdots\pm a_k)^{p^n}\pm a_{k+1}^{p^n}=\left(a_1^{p^n}\pm a_2^{p^n}\pm\cdots\pm a_k^{p^n}\right)\pm a_{k+1}^{p^n}$$

$$=a_1^{p^n}\pm a_2^{p^n}\pm\cdots\pm a_k^{p^n}\pm a_{k+1}^{p^{k+1}}.$$

由归纳原理，命题成立.

4) $(n1)^p=(\overbrace{1+1+\cdots+1}^{n\text{个}})^p=\overbrace{1^p+1^p+\cdots+1^p}^{n\text{个}}=\overbrace{1+1+\cdots+1}^{n\text{个}}=n1.$

5) $(a-b)^p=(a-b)(a-b)^{p-1}$. 又

$$(a-b)^p=a^p-b^p=(a-b)\left(a^{p-1}+a^{p-2}b+\cdots+ab^{p-2}+b^{p-1}\right),$$

从而

$$(a-b)(a-b)^{p-1}=(a-b)\left(a^{p-1}+a^{p-2}b+\cdots+ab^{p-2}+b^{p-1}\right).$$

① 当 $a-b\neq 0$ 时，因 R 无零因子，故消去律成立，于是

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 96. 22 行.

$$(a-b)^{p-1}=a^{p-1}+a^{p-2}b+\cdots+ab^{p-2}+b^{p-1}.$$

② 当 $a-b=0$ 即 $a=b$ 时，因 $\mathrm{ch}\,R=p$，故

$$a^{p-1}+a^{p-2}b+\cdots+ab^{p-2}+b^{p-1}=pa^{p-1}=0=(a-b)^{p-1}.$$

注 1) **注意，R 必须是交换环，命题才成立.**

2) 1963 年卡斯拉(S. Caslar)证明了命题：设 R 是特征为素数 p 的除环，则

$$R \text{ 是域} \Leftrightarrow \forall a,b\in R,(a+b)^p=a^p+b^p$$

的充分性.

5. 利用上面 4 题证明：在 $\mathbb{Z}_7$ 中，

1) $[5^7]=[2^8]+[1]$；

2) $[5^7]=[5]$.

证 $\mathbb{Z}_7$ 是无零因子的交换环，且 $\mathrm{ch}\,\mathbb{Z}_7=7$.

1) $[5^7]=[5]^7=([2]+[2]+[1])^7=[2]^7+[2]^7+[1]^7=2[2^7]+[1]=[2^8]+[1]$.

2) $[5^7]=[5]^7=([1]+[1]+[1]+[1]+[1])^7=[1]^7+[1]^7+[1]^7+[1]^7+[1]^7=[1]+[1]+[1]+[1]+[1]=[5]$.

四、思考问题

1. 试判断以下各集 F 对于规定的＋、· 来说是否作成域.

1) $F=\left\{\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \middle| a,b\in\mathbf{Q}\right\}$. ＋：矩阵加法，·：矩阵乘法.

2) $F=\left\{\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \middle| a,b\in\mathbf{R}\right\}$. ＋：矩阵加法，·：矩阵乘法.

3) $F=\left\{a+b\sqrt[3]{5}+c\sqrt[3]{25} \middle| a,b,c\in\mathbf{Q}\right\}$. ＋：实数加法，·：实数乘法.

4) $F\left\{\dfrac{p(x)}{q(x)}=\dfrac{a_0+a_1x+\cdots+a_nx^n}{b_0+b_1x+\cdots+b_mx^m} \middle| a_i,b_j\in\mathbf{Q},q(x)\neq 0\right\}$.

$$\frac{p(x)}{q(x)}=\frac{r(x)}{s(x)}\Leftrightarrow p(x)s(x)=r(x)q(x),$$

$$\frac{p(x)}{q(x)}+\frac{r(x)}{s(x)}=\frac{p(x)s(x)+r(x)q(x)}{q(x)s(x)},$$

$$\frac{p(x)}{q(x)}\cdot\frac{r(x)}{s(x)}=\frac{p(x)r(x)}{q(x)s(x)}.$$

2. 设 R 是除环．证明：加群 R 与乘群 $R^*=R-\{0\}$ 不同构.

3. 设 R 是含 q 个元的有限除环. 证明：$\forall a\in R, a^q=a$.

4. 设 R 是环，$a\in R$. 若 $\exists b\in R$，使得 $a+b-ab=0$，则称 b 为 a 的右拟逆元．证明：除环 R 中的元除单位元 1 外，其余的元都有右拟逆元.

5. 证明：不存在只含 6 个元的整环.

6. 设 F 是含 5 个元的域．证明：

1) $\mathrm{ch}\,F=5$

2) 乘群 $F^*=F-\{0\}$ 是一个 4 阶循环群．(参看第十七章，一，9).

第十一章　子环、环的同态、多项式环

一、基本问题问答

1. 子环、子整环、子除环和子域的定义是什么？并给出一些判别条件.

答　1)　设 R 是环，则

S 是环 R 的子环（R 称为 S 的扩环）$\overset{\text{定义}}{\Longleftrightarrow}$ ① $S\subset R$；

② S 对于 R 的 $+$、$\cdot$ 来说作成一个环

$\Leftrightarrow$ ① $\varnothing\neq S\subset R$；

② $\forall a,b\in S\Rightarrow a-b\in S$；

③ $\forall a,b\in S\Rightarrow ab\in S$

$\Leftrightarrow$ ① $\varnothing\neq S\subset R$；

② $\forall a,b\in S\Rightarrow a+b,-a,ab\in S$.

2)　设 R 是整环，则

S 是整环 R 的子整环 $\overset{\text{定义}}{\Longleftrightarrow}$ ① $S\subset R$；

② S 对于 R 的 $+$、$\cdot$ 来说作成一个整环

$\Leftrightarrow$ ① $S\subset R$；

② $\forall a,b\in S\Rightarrow a-b\in S$；

③ $\forall a,b\in S\Rightarrow ab\in S$；

④ S 有单位元.

3)　设 R 是除环，则

S 是除环 R 的子除环 $\overset{\text{定义}}{\Longleftrightarrow}$ ① $S\subset R$；

② S 对于 R 的 $+$、$\cdot$ 来说作成一个除环

$\Leftrightarrow$ ① $S\subset R$；

② S 中有非零元；

③ $\forall a,b\in S\Rightarrow a-b\in S$；

④ $\forall a,b\in S,b\neq 0\Rightarrow ab^{-1}\in S$

$\Leftrightarrow$ ① $S\subset R$；

② $\forall a,b\in S\Rightarrow a-b\in S$；

③ $S^{*}=S-\{0\}$ 是乘群

$\Leftrightarrow$ ① $S\subset R$；

② S 中有非零元；

③ $\forall a,b,c(\neq 0)\in S\Rightarrow a-b,ab,c^{-1}\in S$

$\Leftrightarrow$ ① S 是 R 的非零子环；

② $\forall a\in S, a\neq 0 \Rightarrow a^{-1}\in S$.

4）设 F 是域，则

S 是域 F 的子域（称 F 为 S 的扩域）$\overset{\text{定义}}{\Longleftrightarrow}$ ① $S\subset F$；

② S 对于 F 的＋、· 来说作成一个域

$\Leftrightarrow$ ① $S\subset F$；

② S 中有非零元；

③ $\forall a,b\in S \Rightarrow a-b\in S$；

④ $\forall a,b\in S, b\neq 0 \Rightarrow ab^{-1}\in S$.

5）设 F 是有限域，则

S 是 F 的子域 $\Leftrightarrow$ ① $S\subset F$；

② S 至少有两个元；

③ $\forall a,b\in S \Rightarrow a+b, ab\in S$.

命题 5）由第十章，二，3 可证.

2. 什么是环 R 的当然子环、真子环？什么是域 F 的当然子域、真子域？

答　环 R 与零环 $\{0\}$ 是 R 的当然子环. 若 S 是 R 的子环，但 $S\neq R$ 且 $S\neq\{0\}$，则称 S 是 R 的真子环.

域 F 是 F 的当然子域. 若 S 是 F 的子域，但 $S\neq F$，则称 S 为 F 的真子域.

环 R 的当然子环与域 F 的当然子域必存在.

3. 设 S 是环 R 的子环，举例说明：

1）可能 R 与 S 都无单位元.

2）可能 R 无单位元而 S 有单位元.

3）可能 R 有单位元而 S 无单位元.

4）可能 R 与 S 都有单位元，而

① R 与 S 的单与元不相同.

② R 与 S 的单位元相同.

5）若 S' 也是环 R 的子环，R,S,S' 都有单位元，可能三者各不相同.

答　1）$4\mathbb{Z}=\{4n \mid n\in\mathbb{Z}\}$ 是偶数环 $2\mathbb{Z}=\{2n \mid n\in\mathbb{Z}\}$ 的子环，二者都无单位元.

2）$S=\left\{\begin{pmatrix} a & 0\\ a & 0\end{pmatrix} \middle| a\in\mathbb{C}\right\}$ 是环 $R=\left\{\begin{pmatrix} a & 0\\ b & 0\end{pmatrix} \middle| a,b\in\mathbb{C}\right\}$ 的子环，R 无单位元，S 有单位元 $\begin{pmatrix} 1 & 0\\ 1 & 0\end{pmatrix}$.

3）设 $\mathbb{Z}_2=\{[0],[1]\}=\{0,1\}$，则 $S=\left\{\begin{pmatrix} 0 & 0\\ 0 & 0\end{pmatrix},\begin{pmatrix} 1 & 1\\ 0 & 0\end{pmatrix},\begin{pmatrix} 1 & 0\\ 0 & 0\end{pmatrix},\begin{pmatrix} 0 & 1\\ 0 & 0\end{pmatrix} \middle| 0,1\in\mathbb{Z}_2\right\}$ 是环 $M_2(\mathbb{Z}_2)$ 的子环，$M_2(\mathbb{Z}_2)$ 有单位元 $\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}$，$S$ 无单位元. 又例，$S=$

$\left\{(a_{ij})\middle|(a_{ij})\in M_n(\mathbb{Z});\forall i\leqslant j,a_{ij}=0\right\}$是$M_n(\mathbb{Z})$的子环，$M_n(\mathbb{Z})$有单位元$\begin{pmatrix}1&&&\\&1&&\\&&\ddots&\\&&&1\end{pmatrix}$，

但S无单位元，因为，取$A=\begin{pmatrix}0&0&\cdots&0\\\vdots&\vdots&&\vdots\\0&0&\cdots&0\\1&0&\cdots&0\end{pmatrix}\in S$，$\forall X=\begin{pmatrix}0&0&\cdots&0&0\\a_{21}&0&\cdots&0&0\\\vdots&\vdots&&\vdots&\vdots\\a_{n1}&a_{n2}&\cdots&a_{n,n-1}&0\end{pmatrix}\in$ S，有$XA=0\neq A$，即S中任意元都不能是左单位元. 所以，S无单位元.

4) ① $S=\left\{(a_{ij})\middle|(a_{ij})\in M_n(\mathbb{Z});a_{in}=a_{nj}=0,i,j=1,2,\cdots,n\right\}$是环$M_n(\mathbb{Z})$的子环.

$M_n(\mathbb{Z})$有单位元$\begin{pmatrix}1&&&&\\&1&&&\\&&\ddots&&\\&&&1&\\&&&&1\end{pmatrix}$，$S$有单位元$\begin{pmatrix}1&&&&\\&1&&&\\&&\ddots&&\\&&&1&\\&&&&0\end{pmatrix}$，二者不相同. 又例，$S=\{0\}$是整数环$\mathbb{Z}$的子环，但$S$的单位元0不等于$\mathbb{Z}$的单位元1.

② $\mathbb{Z}$是环$\mathbb{Z}[\mathrm{i}]=\left\{a+b\mathrm{i}\middle|a,b\in\mathbb{Z}\right\}$的子环，二者的单位元都是数1. 又例，数域$F$是$F$上多项式环$F[x]$的子环，二者的单位元都是数1.

5) $S=\{[0],[3]\}$与$S'=\left\{[0],[2],[4]\right\}$都是模6的剩余类环$\mathbb{Z}_6$的子环. $\mathbb{Z}_6$有单位元$[1]$，S有单位元$[3]$，S'有单位元$[4]$，它们各不相同.

注 环与其子环在是否有单位元的问题上没有必然的规律. 各种情况都可能发生.

4. 试判断下列各命题是否正确. 设S是环R的子环.

1) S的零元与R的零元相同.

2) S中任意元a在S中的负元与a在R中的负元相同.

3) 若R无零因子，则S也无零因子.

4) 若R有零因子，则S也有零因子.

5) 若R与S有相同的单位元，则

① 如果a是S的可逆元，那么a也是R的可逆元.

② 如果$a\in S$，a是R的可逆元，那么a也是S的可逆元.

6) 若R与S都有单位元，但二者不相同. 如果a是S的可逆元，那么a一定不是R的可逆元.

答 1) 正确. 因为S是加群R的子加群.

2) 正确.

3) 正确. 即：若S有零因子a，则R也有零因子a.

4) 不正确. 例，$\mathbb{Z}_6$有零因子，但$\mathbb{Z}_6$的子环$S=\{[0],[3]\}$无零因子.

5) ① 正确. 而且，a在S的逆元与a在R的逆元相同.

② 不正确. 例，$\mathbb{Z}$是$\mathbb{Q}$的子环，它们有相同的单位元1. $3\in\mathbb{Z}$，3是$\mathbb{Q}$的可逆元，但3不是$\mathbb{Z}$的可逆元.

6)　正确. 事实上，当 $a=0$ 时，因 a 是 S 的可逆元，故 $S=\{0\}$，此时 S 的单位元是 0，由已知条件，$R\neq\{0\}$，从而 $a=0$ 不是 R 的可逆元. 当 $a\neq 0$ 时，设 1 与 $1'$ 分别是 R 与 S 的单位元且 $1\neq 1'$. 假定 a 是 R 的可逆元，则由第九章，三，1，3)，①知，a 不是 R 的零因子. 因 $a\in S$，故 $1a=1'a=a$，从而 $(1-1')a=0$. 由 $a\neq 0$，a 不是 R 的零因子，有 $1-1'=0$，即 $1=1'$，此与 $1\neq 1'$ 矛盾. 所以 a 不是 R 的可逆元.

由上面证明可见：若环 R 与其子环 S 都有单位元，但二者不相同. 如果 a 是 R 的可逆元，假定 $a\in S$，就要产生矛盾，因此 a 一定不在 S 中.

5. 试判断下列各命题是否正确.

1)　整环与其子整环的单位元相同.

2)　除环(域)与其子除环(子域)的单位元相同.

3)　设 $S(\neq\{0\})$ 是整环(除环、域) R 的子整环(子除环、子域). 若 a 是 S 的可逆元，则 a 在 S 中的逆元 a' 与 a 在 R 中的逆元 a^{-1} 相同.

答　1)　不正确. 例，整环 $\mathbf{Z}$ 与其子整环 $\{0\}$ 的单位元分别是 1 与 0，二者不相同. 但整环 R 与其子整环 $S(\neq\{0\})$ 的单位元却是相同的. 事实上，设 R 与 S 的单位元分别是 1 与 $1'$. 因 $S\neq\{0\}$，故 $\exists\ a\in S, a\neq 0$，使得 $1'a=a=1a$. 由消去律，$1'=1$.

2)　正确. 事实上，设 S 是除环 R 的子除环，则 $S^*=S-\{0\}$ 是乘群 $R^*=R-\{0\}$ 的子乘群，从而 S^* 与 R^* 的单位元相同，即 S 与 R 有相同的单位元.(或者，利用本题 1)中的方法，也可证明该命题.)

3)　正确. 事实上，因 S 与 R 的单位元相同，故 $aa'=aa^{-1}=1$，即 $a(a'-a^{-1})=0$. 又 $a\neq 0$，由消去律，$a'=a^{-1}$.

6. 设 1)　R_0 是有单位元的交换环；　2)　R 是 R_0 的子环；　3)　R 含 R_0 的单位元；　4)　取定 $\alpha\in R_0$. 证明：

$$R[\alpha]=\left\{f(\alpha)=a_0+a_1\alpha+\cdots+a_n\alpha^n\ \middle|\ a_i\in R, n\text{ 是非负整数}\right\}$$

是含 R 和 α 的 R_0 的最小子环. 特别指明已知条件用在证明中的何处.

证　1)　首先证明 $R[\alpha]$ 是 R_0 的子环.

$\forall f(\alpha)=a_0+a_1\alpha+\cdots+a_n\alpha^n\in R[\alpha]$. 因 R 是环 R_0 的子环，$\alpha\in R_0$，故 $f(\alpha)\in R_0$，从而 $R[\alpha]\subset R_0$. 因 $0+0\alpha+\cdots+0\alpha^n=0\in R[\alpha]$，故 $R[\alpha]\neq\varnothing$. $\forall f(\alpha), g(\alpha)\in R[\alpha]$，设 $f(\alpha)=a_0+a_1\alpha+\cdots+a_n\alpha^n$，$g(\alpha)=b_0+b_1\alpha+\cdots+b_m\alpha^m$，则 $-g(\alpha)=-b_0-b_1\alpha-\cdots-b_m\alpha^m\in R[\alpha]$. 不妨设 $n\geqslant m$，因 R_0 是环，故

$$\begin{aligned}&f(\alpha)-g(\alpha)\\&=f(\alpha)+(-g(\alpha))\\&=(a_0-b_0)+(a_1-b_1)\alpha+\cdots+(a_m-b_m)\alpha^m+a_{m+1}\alpha^{m+1}+\cdots+a_n\alpha^n\in R[\alpha].\end{aligned}$$

因 R_0 是交换环，R 是环，故

$$f(\alpha)g(\alpha)=c_0+c_1\alpha+\cdots+c_{n+m}\alpha^{n+m},$$

其中

$$c_k=a_0b_k+a_1b_{k-1}+\cdots+a_kb_0=\sum_{i+j=k}a_ib_j\in R,$$

$k=0,1,2,\cdots,n+m$，从而 $f(\alpha)g(\alpha)\in R[\alpha]$. 所以 $R[\alpha]$ 是 R_0 的子环.

2)　$\forall a\in R$，$a=a+0\alpha+\cdots+0\alpha^n\in R[\alpha]$，从而 $R\subset R[\alpha]$.

3)　因 R 的单位元 1 就是 R_0 的单位元，故 $\alpha=1\alpha=0+1\alpha+0\alpha^2+\cdots+0\alpha^n\in R[\alpha]$.

4) 设 S 是含 R 和 α 的 R_0 的一个子环，则 $\forall f(\alpha)=a_0+a_1\alpha+\cdots+a_n\alpha^n\in R[\alpha]$，因 $\alpha\in S$，$a_i\in R\subset S$ 且 S 是环，故 $f(\alpha)=a_0+a_1\alpha+\cdots+a_n\alpha^n\in S$，从而 $R[\alpha]\subset S$.

综上可知，$R[\alpha]$是含 R 和 α 的 R_0 的最小子环.

注 1) 由 $\alpha\in R[\alpha]$知，α 是 R 上 α 的多项式. 由 $R\subset R[\alpha]$知，R 中元都是 R 上 α 的多项式.

2) 由已知条件：R 含 R_0 的单位元 1，才能保证 $\alpha=1\alpha=0+1\alpha+0\alpha^2+\cdots+0\alpha^n\in R[\alpha]$. 否则，若 R 的单位元 $1'$ 不是 R_0 的单位元 1，则未必有 $\alpha=1'\alpha$. 例，子环 $R=\left\{\begin{pmatrix}a&0\\0&0\end{pmatrix}\middle|\,a\in\mathbf{Q}\right\}$的单位元 $1'=\begin{pmatrix}1&0\\0&0\end{pmatrix}$不是环 $R_0=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\middle|\,a,b,c,d\in\mathbf{Q}\right\}$的单位元 $1=\begin{pmatrix}1&0\\0&1\end{pmatrix}$，显然，$1'\begin{pmatrix}a&b\\c&d\end{pmatrix}=\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}=\begin{pmatrix}a&b\\0&0\end{pmatrix}\neq\begin{pmatrix}a&b\\c&d\end{pmatrix}$（当 c,d 不同时为 0 时）.

3) 假设下文出现的环 R_0 与环 R 都具有该命题中的条件 1),2),3).

7. 举例说明可能环 R 上 α 的多项式环 $R[\alpha]$中有的元表法不唯一.

答

例 1 取定 $\alpha\in R$，显然 $0\in R[\alpha]$，有

$$0=0+0\alpha,\quad 0=\alpha+(-1)\alpha,$$

即 0 表成 α 的多项式的形式不唯一.

例 2 $R=\{0,1\}$对于

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

作成一个有单位元 1 的交换环. 若取定 $\alpha=1\in R$，显然 $0\in R[\alpha]$，有

$$0=1+\alpha,\quad 0=1+\alpha^2,$$

即 0 表成 α 的多项式的形式不唯一. 若取定 $\alpha=0\in R$，显然 $1\in R[\alpha]$有

$$1=1+\alpha,\quad 1=1+\alpha^2,$$

即 1 表成 α 的多项式的形式也不唯一.

例 3 $\mathbf{Z}$ 上$\sqrt{2}$的多项式环 $\mathbf{Z}[\sqrt{2}]$中元 0 既可表成系数全为 0 的$\sqrt{2}$的多项式：$0=0+0\sqrt{2}+0(\sqrt{2})^2$，也可表成系数不全为 0 的$\sqrt{2}$的多项式：$0=-2+(\sqrt{2})^2$.

注 环 $R[\alpha]$中的元表法不唯一，这会给我们带来许多麻烦. 为了使表法唯一，就需要强化条件，引出 R 上未定元的概念.

8. 环 R 上未定元的定义是什么？环 R 上未定元 x 的多项式 $f(x)$的主要特点是什么？

答

$x(\in R_0)$是 R 上的一个未定元

$\Leftrightarrow x\in R_0$，$\overline{\exists}$不全为 0 的元 $a_0,a_1,a_2,\cdots,a_n\in R$，使得

$$a_0+a_1x+a_2x^2+\cdots+a_nx^n=0$$

$\Leftrightarrow x\in R_0$，若 R 上 x 的多项式 $a_0+a_1x+a_2x^2+\cdots+a_nx^n=0$，则系数 $a_0=a_1=a_2=\cdots=a_n=0$（即零多项式的表法唯一）.

环 R 上未定元 x 的多项式 $f(x)$ 的主要特点是 $f(x)$ 的表法唯一. 事实上，$\forall f(x)\in R[x]$，若 $f(x)=a_0+a_1x+\cdots+a_nx^n+a_{n+1}x^{n+1}+\cdots+a_mx^m=b_0+b_1x+\cdots+b_nx^n$，其中 $n\leqslant m$，则

$$(a_0-b_0)+(a_1-b_1)x+\cdots+(a_n-b_n)x^n+a_{n+1}x^{n+1}+\cdots+a_mx^m=0.$$

因 x 是 R 上未定元，故

$$a_i=b_i, i=0,1,\cdots,n \text{ 且 } a_{n+1}=\cdots=a_m=0,$$

从而 $f(x)$ 的表法唯一.

注　1)　由零多项式的表法唯一可证明，任一多项式的表法都唯一. 而环 R 上未定元 x 的多项式 $f(x)$ 表法唯一，即 $f(x)$ 的系数随 $f(x)$ 唯一确定，这样才能得出多项式环 $R[x]$ 中的很好的结果. 环 R 上的非未定元 α 的多项式环 $R[\alpha]$ 的代数结构就比较复杂.

2)　《高等代数》[①]中讨论的数域 F 上的一元多项式 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$ 就是数域 F 上未定元 x 的多项式，$f(x)$ 的表法唯一. 但是当时有些问题是含糊不清的. 比如，x 总使我们感到神秘，它究竟是什么？又如，$f(x)$ 的表达式中出现的乘法与加法究竟是什么意思？至此，这些问题就彻底解决了.

9. 举例说明，对于给定的有单位元的交换环 R_0 来说，R_0 未必含有环 R 上的未定元.

答　例，设 $R_0=\left\{a+b\sqrt{2}\,\middle|\,a,b\text{ 是有理数}\right\}$ 是有单位元 1 的交换环. R=有理数环是 R_0 的一个子环，且含 R_0 的单位元 1. 那么 R_0 中不含 R 上的未定元. 事实上，$\forall \alpha=a+b\sqrt{2}\in R_0$，有

$$(a^2-2b^2)+(-2a)\alpha+1\alpha^2=0,$$

其中 $1\neq 0$. 所以 R_0 中任意元 α 不是 R 上的未定元.

注　给出有单位元的交换环 R 以后，由未定元存在定理[②]，我们总可以造出一个有单位元 1 的交换环 P，使 R 是 P 的子环，1 即为 R 的单位元，且在 P 中存在 R 上的未定元. 从而 R 上未定元 x 必存在.

10. 回答下列问题.

1)　$R[0]=?$　　$R[1]=?$

2)　为何不类似于未定元多项式的次数定义来定义环 R 上非未定元 α 的多项式 $f(\alpha)$ 的次数？

3)　在《高等代数》[③]中对于数域 F 上一元多项式 $f(x)$，可以看成变量 $x(\in F)$ 的函数. 因为这时把 $f(x)$，$g(x)$ 看成多项式，它们相等与把 $f(x)$，$g(x)$ 看成函数，它们相等是一致的. 现在对于有单位元的交换环 R 上的一元多项式 $f(x)$ 来说，能否将 $f(x)$ 看成变量 $x(\in R)$ 的函数？

答　1)　$R[0]=R$.　$R[1]=R$.

2)　因为 $f(\alpha)$ 的表法未必唯一. 例，$f(i)=1+4i+3i^2+4i^3+2i^4$ 是整数环 $\mathbb{Z}$ 上的多项式. 又 $f(i)=0$，那么 $f(i)$ 的次数是 4 还是不存在呢？无法唯一确定.

3)　不能. 例，取 R 为 $\mathbb{Z}_2=\{[0],[1]\}$，$f(x)=x+[1]$，$g(x)=x^2+[1]$ 是 $\mathbb{Z}_2$ 上的一元多项式. 显然 $f(x)\neq g(x)$. 但是，若把 $f(x)$，$g(x)$ 看成 $x(\in\mathbb{Z}_2)$ 的函数，取 $x=[0]$ 时，

---

①③ 北京大学数学系几何与代数教研室. 高等代数. 北京：高等教育出版社，1978

② 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 103. 定理.

$f([0])=g([0])=[1]$. 取 $x=[1]$时，$f([1])=g([1])=[0]$，因此 x 取遍 $\mathbb{Z}_2$ 中的元时，函数值都分别相等，从而函数 $f(x)$ 与函数 $g(x)$ 相等.

二、典型问题分析

1. 证明：一个环的中心是一个交换子环.

证 设 $N=\{n\in \text{环} R \mid \forall a\in R, an=na\}$ 是环 R 的中心. 因 $0\in R$ 且 $\forall a\in R, a0=0=0a$，故 $0\in N$，从而 $N\neq\varnothing$. 显然 $N\subset R$. $\forall n_1,n_2\in N, \forall a\in R$，有

$$(n_1-n_2)a=n_1a-n_2a=an_1-an_2=a(n_1-n_2),$$

$$(n_1n_2)a=n_1(n_2a)=n_1(an_2)=(n_1a)n_2=(an_1)n_2=a(n_1n_2),$$

从而 $n_1-n_2, n_1n_2\in N$. 于是 N 是 R 的子环.

$\forall n_1,n_2\in N$，必有 $n_2\in R$，由中心定义，$n_1n_2=n_2n_1$. 所以 N 是 R 的交换子环.

注 R 是交换环 $\Leftrightarrow$ 环 R 的中心 $=R$.

2. 证明：一个除环的中心是一个域.

证一 由上面题 1 知，除环 R 的中心 N 是 R 的交换子环，因 R 是除环，故 $1(\neq 0)\in R$ 且 $\forall a\in R, a1=a=1a$，从而 $1\in N$. $\forall n\in N, n\neq 0, \forall a\in R$，有 $na=an$. 因 R 是除环，故 n 有逆元 $n^{-1}\in R$，使得 $n^{-1}nan^{-1}=n^{-1}ann^{-1}$，即 $an^{-1}=n^{-1}a$.（或可如下证明：$an^{-1}=n^{-1}nan^{-1}=n^{-1}ann^{-1}=n^{-1}a$.）从而 $n^{-1}\in N$. 所以 N 是一个域.

证二 已知除环 R 的中心 N 是 R 的交换子环. N 含不等于零的元 1. $\forall n_1,n_2\in N$, $n_2\neq 0$, $\exists n_2^{-1}\in R, \forall a\in R$，有

$$(n_1n_2^{-1})a=(n_1n_2^{-1})a(n_2n_2^{-1})=n_1n_2^{-1}n_2an_2^{-1}=n_1an_2^{-1}=a(n_1n_2^{-1}),$$

从而 $n_1n_2^{-1}\in N$. 于是 N 是 R 的子除环. 所以 N 是域.

证三 已知除环 R 的中心 N 是 R 的交换子环. 因 R 是除环，故 $R^*=R-\{0\}$ 是乘群. 因 $N^*=N-\{0\}$ 是 R^* 的中心，故 N^* 是 R^* 的子群[①]，即 N^* 是乘群，又已知 N 是交换环，所以 N 是域.

3. 证明：有理数域 $\mathbb{Q}$ 是所有复数 $a+bi(a,b$ 是有理数$)$ 作成的域 $\mathbb{Q}(i)$ 的唯一的真子域.

证 因 $\mathbb{Q}\subset\mathbb{Q}(i)$ 且 $\mathbb{Q}$ 对于 $\mathbb{Q}(i)$ 的 $+$、$\cdot$ 来说作成一个域，故 $\mathbb{Q}$ 是 $\mathbb{Q}(i)$ 的子域[②]. 又 $i\in\mathbb{Q}(i)$，但 $i\overline{\in}\mathbb{Q}$，从而 $\mathbb{Q}$ 是 $\mathbb{Q}(i)$ 的真子域.

下面证明 $\mathbb{Q}$ 是 $\mathbb{Q}(i)$ 的唯一的真子域. 设 F 是 $\mathbb{Q}(i)$ 的任一子域. 由《高等代数》[③]知，有理数域 $\mathbb{Q}$ 是最小数域，从而

$$\mathbb{Q}\subset F\subset\mathbb{Q}(i).$$

只需证明：$F=\mathbb{Q}$ 或 $F=\mathbb{Q}(i)$. 若 $F=\mathbb{Q}$，则命题已证. 若 $F\neq\mathbb{Q}$，又因 $F\subset\mathbb{Q}(i)$，故 $\exists u+vi\in F-\mathbb{Q}$，其中 u,v 是有理数且 $v\neq 0$. 因 $F\supset\mathbb{Q}$，故 $-u\in F, v^{-1}=\dfrac{1}{v}\in F$. 又 F 是域，有 $\dfrac{1}{v}[(u+vi)-u]=i\in F$. $\forall a+bi\in\mathbb{Q}(i), a,b\in\mathbb{Q}$，因此 $a,b\in F$. 又 $i\in F$ 且 F 是域，从而 $a+bi\in F$,

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 71. 例 2.

② 同上. 97. 定义.

③ 北京大学数学系几何与代数教研室. 高等代数. 北京：高等教育出版社，1978

即$\mathbb{Q}(\mathrm{i})\subset F$，已知$F\subset\mathbb{Q}(\mathrm{i})$，所以$F=\mathbb{Q}(\mathrm{i})$.

注　有理数域$\mathbb{Q}$是最小数域. 事实上，设F是任一数域，则$1,0\in F$，从而任意正整数$n=\overbrace{1+1+\cdots+1}^{n个}\in F$且$-1\in F$. 于是任意负整数$-n=n(-1)\in F$. 至此，全体整数都在$F$中. 设$\frac{n}{m}$是任意有理数，其中$n,m$是整数且$m\neq 0$，从而$m^{-1}=\frac{1}{m}\in F$. 因此$\frac{n}{m}=nm^{-1}\in F$. 所以$\mathbb{Q}\subset F$.

4. 证明：$\mathbb{Q}(\mathrm{i})$有且只有两个自同构映射.

证　设ϕ是$\mathbb{Q}(\mathrm{i})$的任意一个自同构，则$\phi(0)=0,\phi(1)=1$①. 对于任意正整数n，有

$$\phi(n)=\phi(\overbrace{1+1+\cdots+1}^{n个})=\overbrace{\phi(1)+\phi(1)+\cdots+\phi(1)}^{n个}=\overbrace{1+1+\cdots+1}^{n个}=n,$$
$$\phi(-n)=-\phi(n)=-n.$$

所以任意整数在自同构下的象都是本身.

$\forall\frac{a}{b}\in\mathbb{Q}$，其中$a,b\in\mathbb{Z},b\neq 0$，因$\phi$是自同构，故$\phi(b^{-1})=[\phi(b)]^{-1}=b^{-1}$，从而

$$\phi(\frac{a}{b})=\phi(ab^{-1})=\phi(a)\phi(b^{-1})=ab^{-1}=\frac{a}{b}.$$

所以任意有理数在自同构下的象都是本身.

设$\phi(\mathrm{i})=x$，则$\phi(\mathrm{i}^2)=x^2$. 又$\phi(\mathrm{i}^2)=\phi(-1)=-1$，从而$x^2=-1$，即$x=\pm\mathrm{i}$，于是$\phi(\mathrm{i})=\pm\mathrm{i}$.

当$\phi(\mathrm{i})=\mathrm{i}$时，$\forall\alpha=a+b\mathrm{i}\in\mathbb{Q}(\mathrm{i})$，有$\phi(\alpha)=\phi(a+b\mathrm{i})=\phi(a)+\phi(b)\phi(\mathrm{i})=a+b\mathrm{i}=\alpha$，此时$\phi$是$\mathbb{Q}(\mathrm{i})$的恒等自同构.

当$\phi(\mathrm{i})=-\mathrm{i}$时，$\forall\alpha=a+b\mathrm{i}\in\mathbb{Q}(\mathrm{i})$，有$\phi(\alpha)=\phi(a+b\mathrm{i})=\phi(a)+\phi(b)\phi(\mathrm{i})=a-b\mathrm{i}=\bar{\alpha}$

显然共轭变换ϕ是$\mathbb{Q}(\mathrm{i})$与$\mathbb{Q}(\mathrm{i})$间的一个一一映射，且$\forall\alpha,\beta\in\mathbb{Q}(\mathrm{i})$有

$$\phi(\alpha+\beta)=\overline{\alpha+\beta}=\bar{\alpha}+\bar{\beta}=\phi(\alpha)+\phi(\beta),$$
$$\phi(\alpha\beta)=\overline{\alpha\beta}=\bar{\alpha}\,\bar{\beta}=\phi(\alpha)\,\phi(\beta).$$

所以，此时ϕ是$\mathbb{Q}(\mathrm{i})$的一个自同构.

综上可知，$\mathbb{Q}(\mathrm{i})$有且只有两个自同构：恒等自同构和共轭自同构.

注　1)　仿该命题的证法，可证明整数环$\mathbb{Z}$与有理数域$\mathbb{Q}$的自同构都有且只有恒等自同构：$a\to a$. 而映射：$a\to -a$是整数加群与有理数加群的自同构，但不是整数环与有理数域的自同构.

2)　环R到自身的同态映射叫做环R的自同态. 整数环$\mathbb{Z}$与有理数域$\mathbb{Q}$的自同态都有且只有零同态$\phi_1:a\to 0$和恒等自同态$\phi_2:a\to a$. 事实上，ϕ_1和ϕ_2显然都是$\mathbb{Z}$与$\mathbb{Q}$的自同态. 设ϕ是$\mathbb{Z}$的任一自同态. 设$\phi(1)=n$，则

$$n^2=[\phi(1)]^2=\phi(1)\,\phi(1)=\phi(1\cdot 1)=\phi(1)=n.$$

即　$n(n-1)=0$. 因$\mathbb{Z}$无零因子，故$n=1$或$n=0$.

当$\phi(1)=0$时，$\forall a\in\mathbb{Z}$，$\phi(a)=\phi(a1)=\phi(a)\phi(1)=\phi(a)0=0$，所以此时，$\phi$是$\mathbb{Z}$的零同态.

---

①　张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 98. 定理 2.

当 $\phi(1)=1$ 时，$\forall a\in\mathbb{Z}$. 若 $a>0$，则 $\phi(a)=\phi(\overbrace{1+1+\cdots+1}^{a个})=\overbrace{\phi(1)+\phi(1)+\cdots+\phi(1)}^{a个}=\overbrace{1+1+\cdots+1}^{a个}=a$；若 $a<0$，则 $-a>0$，从而 $\phi(-a)=-a$. 又因 ϕ 是自同态. 故 $\phi(-a)=-\phi(a)$，于是 $-\phi(a)=-a$，因而 $\phi(a)=a$；若 $a=0$，显然 $\phi(a)=a$. 所以此时，ϕ 是 $\mathbb{Z}$ 的恒等自同态.

综上可知，$\mathbb{Z}$ 的自同态有且只有零同态和恒等自同态.

设 ψ 是 $\mathbb{Q}$ 的任一自同态. 由前面的证明知 $\psi(1)=0$ 或 1 且当 $\psi(1)=0$ 时，$\forall a\in\mathbb{Q}$，有 $\psi(a)=0$，所以此时，ψ 是 $\mathbb{Q}$ 的零同态. 当 $\psi(1)=1$ 时，$\forall a\in\mathbb{Z}$，有 $\psi(a)=a$，从而 $\forall \frac{a}{b}\in\mathbb{Q}$，其中 $a,b\in\mathbb{Z}$，$b\neq0$，有

$$\psi\left(\frac{a}{b}\right)=\psi(ab^{-1})=\psi(a)\psi(b^{-1})=\psi(a)(\psi(b))^{-1}=ab^{-1}=\frac{a}{b}.$$

所以此时，ψ 是 $\mathbb{Q}$ 的恒等自同态.

综上可知，$\mathbb{Q}$ 的自同态有且只有零同态和恒等自同态.

5. $\mathbb{Z}_3$ 表示模 3 的剩余类所作成的集合. 找出加群 $\mathbb{Z}_3$ 的所有自同构映射，再找出域 $\mathbb{Z}_3$ 的所有自同构映射.

解 设 ϕ 是加群 $\mathbb{Z}_3=\{[0],[1],[2]\}$ 的一个自同构，则 $\phi:[0]\to[0]$①. 所以加群 $\mathbb{Z}_3$ 的所有自同构只可能是

$$\phi_1:[0]\to[0],\ [1]\to[1],\ [2]\to[2],$$
$$\phi_2:[0]\to[0],\ [1]\to[2],\ [2]\to[1].$$

ϕ_1 是加群 $\mathbb{Z}_3$ 的恒等自同构. 下面验证 ϕ_2 也是加群 $\mathbb{Z}_3$ 的自同构. 显然 ϕ_2 是 $\mathbb{Z}_3$ 与 $\mathbb{Z}_3$ 间的一个一一映射. 因

$$\begin{aligned}\phi_2:\ &[0]+[0]=[0]\to[0]=[0]+[0],\\ &[0]+[1]=[1]\to[2]=[0]+[2],\\ &[0]+[2]=[2]\to[1]=[0]+[1],\\ &[1]+[1]=[2]\to[1]=[2]+[2],\\ &[1]+[2]=[0]\to[0]=[2]+[1],\\ &[2]+[2]=[1]\to[2]=[1]+[1].\end{aligned}$$

又加群 $\mathbb{Z}_3$ 是交换群，故 ϕ_2 保持加群 $\mathbb{Z}_3$ 的加法运算. 所以 ϕ_2 是加群 $\mathbb{Z}_3$ 的自同构. 于是 ϕ_1 与 ϕ_2 是加群 $\mathbb{Z}_3$ 的所有自同构.

设 ψ 是域 $\mathbb{Z}_3$ 的一个自同构，则 $\psi:[0]\to[0],[1]\to[1]$. 所以域 $\mathbb{Z}_3$ 有且只有一个恒等自同构：

$$\psi:[0]\to[0],\ [1]\to[1],\ [2]\to[2].$$

注 ϕ_2 保持加群 $\mathbb{Z}_3$ 的加法运算还可如下验证. $\forall x,y\in\mathbb{Z}_3$，

1） 当 x,y 中有 $[0]$ 时，因 $\mathbb{Z}_3$ 的加法可换，故不妨设 $x=[0]$，从而

$$\phi_2(x+y)=\phi_2([0]+y)=\phi_2(y)=[0]+\phi_2(y)=\phi_2([0])+\phi_2(y)=\phi_2(x)+\phi_2(y).$$

2） 当 $x=y=[1]$ 时，有

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 43. 定理 2.

$$\phi_2(x+y)=\phi_2([1]+[1])=\phi_2([2])=[1]=[2]+[2]=\phi_2([1])+\phi_2([1])$$
$$=\phi_2(x)+\phi_2(y).$$

3)　当 $x=y=[2]$ 时，有

$$\phi_2(x+y)=\phi_2([2]+[2])=\phi_2([1])=[2]=[1]+[1]=\phi_2([2])+\phi_2([2])$$
$$=\phi_2(x)+\phi_2(y).$$

4)　当 x,y 中一个是[1]，另一个是[2]时，$\phi_2(x)$，$\phi_2(y)$ 中一个是[2]，另一个是[1]，于是有

$$\phi_2(x+y)=\phi_2([0])=[0]=[1]+[2]=\phi(x)+\phi(y).$$

以上穷尽了各种情况，因此 ϕ_2 保持加群 $\mathbb{Z}_3$ 的加法运算.

6. 令 R 是四元数除环，$S=\{(a,0)\mid a\text{ 是实数}\}$ 是 R 的子环，$\bar{S}$ 是实数域且 $S\overset{\phi}{\cong}\bar{S}$，其中 $\phi:(a,0)\to a$. 同时 $R-S$ 与 $\bar{S}$ 无公共元.

1)　利用挖补定理或称嵌入定理[①]作出环 $\bar{R}$，使 $R\overset{\psi}{\cong}\bar{R}$ 且 $\bar{S}$ 是 $\bar{R}$ 的子环.

2)　具体写出 R 与 $\bar{R}$ 间的同构映射 ψ.

3)　取 $(\mathrm{i},0),(0,1),(0,\mathrm{i})\in\bar{R}$，令 $(\mathrm{i},0)=i$（左边的 i 是虚数单位 $\sqrt{-1}$，不要与右边的 i 混淆），$(0,1)=j$，$(0,\mathrm{i})=k$，证明 $\bar{R}$ 的每一个元都可写成 $a+bi+cj+dk$（a,b,c,d 是实数）的形式.

4)　验证在 $\bar{R}$ 里有 $i^2=j^2=k^2=-1$，$ij=-ji=k$，$jk=-kj=i$，$ki=-ik=j$.

解　1)

环 $\bar{R}=\{a\in\bar{S};(\alpha,\beta)\in R-S\}$.

$(=\{a\in\bar{S};(\alpha,\beta)\mid\beta\neq0\text{ 或 }\beta=0\text{ 而 }\alpha\text{ 是虚数}\}$

$=\{a\in\bar{S};(\alpha,\beta)\mid\alpha\text{ 是虚数或 }\alpha\text{ 是实数而 }\beta\neq0\}$

$=\{a\in\bar{S};(a+b\mathrm{i},c+d\mathrm{i})\mid a,b,c,d\text{ 是实数},c,d\text{ 不同时为 0 或 }c=d=0\text{ 而 }b\neq0\}$

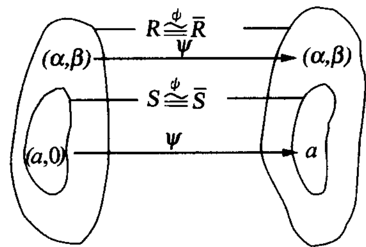
$=\{a\in\bar{S};(a+b\mathrm{i},c+d\mathrm{i})\mid a,b,c,d\text{ 是实数},b\neq0\text{ 或 }b=0\text{ 而 }c,d\text{ 不同时为 0}\})$.

2)　$\forall(\alpha,\beta)\in R$. $(\alpha,\beta)\in S$ 时，

$$\psi:(\alpha,\beta)\to\alpha=\psi((\alpha,\beta))=\phi((\alpha,\beta)).$$

$(\alpha,\beta)\in R-S$ 时，

$$\psi:(\alpha,\beta)\to(\alpha,\beta)=\psi((\alpha,\beta)).$$



由于 $\bar{S}$ 与 $R-S$ 无公共元，仿挖补定理，易证 ψ 是 R 与 $\bar{R}$ 间的一一映射. 规定 $\bar{R}$ 的两个元的和等于它们的逆象的和的象，$\bar{R}$ 的两个元的积等于它们的逆象的积的象[②]，于是这样规定的法则是 $\bar{R}$ 的两个代数运算，而且 ψ 是 R 与 $\bar{R}$ 间的对于一对加法和一对乘法来说的同构映射，即 $R\overset{\psi}{\cong}\bar{R}$. 且 $\bar{S}$ 是 $\bar{R}$ 的子环.

---

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 99. 定理 4.

② 同上. 99. 引理.

3) 取$(\mathrm{i},0)=i,(0,1)=j,(0,i)=k\in\bar{R}$. $\forall a\in\bar{S}\subset\bar{R}$,

$$a=a+0i+0j+0k(\text{在 }\bar{R}\text{ 中的运算}).$$

$\forall(\alpha,\beta)=(a+b\mathrm{i},c+d\mathrm{i})\in R-S\subset\bar{R}$,其中 a,b,c,d 是实数,

$$\begin{aligned}
&(a+b\mathrm{i},c+d\mathrm{i})\\
&\xlongequal{\text{由}\psi\text{的定义}}\psi((a+b\mathrm{i},c+d\mathrm{i}))\\
&\xlongequal{\text{由第十章,二,5}}\psi((a,0)+(b,0)(\mathrm{i},0)+(c,0)(0,1)+(d,0)(0,\mathrm{i}))(\text{在 }R\text{ 中的运算})\\
&\xlongequal[\text{运算}]{\text{由}\psi\text{保持}}\psi((a,0))+\psi((b,0))\psi((\mathrm{i},0))+\psi((c,0))\psi((0,1))+\psi((d,0))\psi((0,\mathrm{i}))\\
&\xlongequal{\text{由}\psi\text{的定义}}a+b(\mathrm{i},0)+c(0,1)+d(0,\mathrm{i})(\text{在 }\bar{R}\text{ 中的运算})\\
&=a+bi+cj+dk.
\end{aligned}$$

所以 $\bar{R}$ 的任意元都可写成$a+bi+cj+dk$(a,b,c,d 是实数)的形式.

4) 在 $\bar{R}$ 里(注意,不是在 R 里)有 $i^2=j^2=k^2=-1,ij=-ji=k,jk=-kj=i,ki=-ik=j$. 事实上,

$$i^2=(\mathrm{i},0)(\mathrm{i},0)=\psi((\mathrm{i},0))\psi((\mathrm{i},0))=\psi((\mathrm{i},0)(\mathrm{i},0))=\psi((-1,0))=-1.$$

同理 $j^2=k^2=-1$.

$$ij=(\mathrm{i},0)(0,1)=\psi((\mathrm{i},0))\psi((0,1))=\psi((\mathrm{i},0)(0,1))=\psi((0,\mathrm{i}))=(0,\mathrm{i})=k,$$

$$\begin{aligned}
-ji&=-(0,1)(\mathrm{i},0)=-\psi((0,1))\psi((\mathrm{i},0))=-\psi((0,1)(\mathrm{i},0))\\
&=-\psi((0,\bar{\mathrm{i}}))=-\psi((0,-\mathrm{i}))=-(0,-\mathrm{i})=(0,\mathrm{i})=k.
\end{aligned}$$

因此 $ij=-ji=k$. 同理 $jk=-kj=i$, $ki=-ik=j$.

注 1) 由本题知

$\bar{R}=\left\{a+bi+cj+dk\,\middle|\,a,b,c,d\text{ 是实数},i^2=j^2=k^2=-1,ij=-ji=k,jk=-kj=i,ki=-ik=j\right\}$

是由实数域所嵌入的四元数除环.

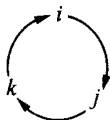
因为 $\forall x\in\bar{R}$,有

$$x=a+bi+cj+dk=a1+bi+cj+dk,$$

其中 a,b,c,d 是实数,即 x 可表成四个元 $1,i,j,k$ 的实系数的线性组合,所以将四元数除环中的元称为四元数.

易证,$\forall x\in\bar{R}$,$x=a+bi+cj+dk$ 的表法唯一.

$\forall x,y\in\bar{R}$,有 $x=a+bi+cj+dk$, $y=a'+b'i+c'j+d'k$. 于是 $x+y=(a+a')+(b+b')i+(c+c')j+(d+d')k$,且 x 与 y 相乘就是根据分配律逐项相乘再合并"同类项". 因此只需掌握 $1,i,j,k$ 间的所有乘法关系,就可求出任意两个元的乘积. 这里 1 是 $\bar{R}$ 的单位元,按照下面箭头顺序.



相邻两元的乘积等于第三个. 若与箭头顺序相反,则相邻两元的乘积等于第三个的负元. i,j,k 自身的平方都等于-1.

$\forall a+bi+cj+dk(\neq 0)\in\bar{R}$,

$$(a+bi+cj+dk)^{-1}=[\psi((a+bi,c+di))]^{-1}=\psi((a+bi,c+di)^{-1})$$
$$=\psi\left[\left(\frac{a-bi}{a^2+b^2+c^2+d^2},\frac{-c-di}{a^2+b^2+c^2+d^2}\right)\right]=\frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}.$$

例，$(1+i-j+k)^{-1}=\frac{1}{4}-\frac{1}{4}i+\frac{1}{4}j-\frac{1}{4}k$.

$\overline{R}'=\{a+bi+cj+dk \mid a,b,c,d\in\mathbb{Q},i^2=j^2=k^2=-1,ij=k=-ji,jk=i=-kj,ki=j=-ik\}$是$\overline{R}$的一个子除环.

在$\overline{R}$中将实数域$\overline{S}$改为复数域$\mathbb{C}$，其余不变，此时$\overline{R}$是一个有零因子的环而不是除环.因为$1+\sqrt{-1}\,j(\neq0)$，$1-\sqrt{-1}\,j(\neq0)\in\overline{R}$.但

$$(1+\sqrt{-1}\,j)(1-\sqrt{-1}\,j)=1-(\sqrt{-1}\,j)^2=1-(-1)j^2=1+(-1)=0.$$

所以$\overline{R}$有零因子.

设$G=\{1,-1,i,-i,j,-j,k,-k\}\subset\overline{R}$，其中1是$G$的单位元，$ij=k=-ji,jk=i=-kj,ki=j=-ik,i^2=j^2=k^2=-1$，则$G$作成一个非交换群.称$G$为四元数群.$G$的全部子群是：单位元群$\{1\}$，1个2阶子群$(-1)$，3个4阶子群$(i)$，$(j)$，$(k)$和$G$本身，因此$G$的所有子群都是不变子群，于是$G$是汉弥尔顿群.此群与第八章，三，10中给出的群同构.

$\overline{R}$的中心Z是实数域$\overline{S}$.事实上，任意实数显然与四元数可换，从而$\overline{S}\subset Z$；反之，$\forall x=a+bi+cj+dk\in Z$，则

$$xi=ai-b-ck+dj\quad,\quad ix=ai-b+ck-dj.$$

因$x\in Z$，故$xi=ix$.于是$-c=c$且$d=-d$，即$c=d=0$.同理由$xj=jx$，可得$b=0$.因此$x=a\in\overline{S}$，从而$Z\subset\overline{S}$.所以$Z=\overline{S}$.

2)　设$K=\left\{\begin{pmatrix}\alpha&\beta\\-\bar\beta&\bar\alpha\end{pmatrix}\middle|\alpha,\beta\in\mathbb{C},\bar\alpha,\bar\beta\text{分别为}\alpha,\beta\text{的共轭复数}\right\}$对于距阵的加法和乘法来说作成一个环.则四元数除环$\overline{R}$与$K$同构.

$$\psi:a+bi+cj+dk\to\begin{pmatrix}a+b\mathrm{i}&c+d\mathrm{i}\\-c+d\mathrm{i}&a-b\mathrm{i}\end{pmatrix}$$

是$\overline{R}$与K间的一个同构映射.

K的子环

$$A_1=\left\{\begin{pmatrix}\alpha&0\\0&\bar\alpha\end{pmatrix}\middle|\alpha\in\mathbb{C}\right\},A_2=\left\{\begin{pmatrix}a&b\\-b&a\end{pmatrix}\middle|a,b\text{是实数}\right\},A_3=\left\{\begin{pmatrix}a&b\mathrm{i}\\b\mathrm{i}&a\end{pmatrix}\middle|a,b\text{是实数}\right\}$$

分别与复数域$\mathbb{C}$同构.

$$\psi_1:\begin{pmatrix}\alpha&0\\0&\bar\alpha\end{pmatrix}\to\alpha\quad,\quad\psi_2:\begin{pmatrix}a&b\\-b&a\end{pmatrix}\to a+b\mathrm{i}\quad,\quad\psi_3:\begin{pmatrix}a&b\mathrm{i}\\b\mathrm{i}&a\end{pmatrix}\to a+b\mathrm{i}$$

分别是A_1,A_2,A_3与$\mathbb{C}$间的同构映射.同样$\overline{R}$的子环

$$B_1=\{a+bi\mid a,b\text{是实数}\},B_2=\{a+cj\mid a,c\text{是实数}\},B_3=\{a+dk\mid a,d\text{是实数}\}$$

也分别与复数域$\mathbb{C}$同构.

$$\psi_1':a+bi\to a+b\mathrm{i}\ (\text{注意左边的 }i=(\mathrm{i},0)\text{，右边的}\mathrm{i}=\sqrt{-1}),$$
$$\psi_2':a+cj\to a+c\mathrm{i},\psi_3':a+dk\to a+d\mathrm{i}$$

分别是 B_1, B_2, B_3 与 $\mathbb{C}$ 间的同构映射.

所以四元数除环是复数域的扩充,或说复数域可扩张为四元数除环.

3) 设 $H=\left\{(a_1,a_2,a_3,a_4)\,\middle|\,a_i \text{ 是实数}, i=1,2,3,4\right\}$, $\forall \alpha=(a_1,a_2,a_3,a_4), \beta=(b_1,b_2,b_3,b_4)\in H$,规定

$$\alpha=\beta \Leftrightarrow a_i=b_i, i=1,2,3,4,$$

$$\alpha+\beta=(a_1+b_1, a_2+b_2, a_3+b_3, a_4+b_4),$$

$$\alpha\beta=(a_1b_1-a_2b_2-a_3b_3-a_4b_4, a_1b_2+a_2b_1+a_3b_4-a_4b_3, a_1b_3+a_3b_1+a_2b_4-a_4b_2, a_1b_4+a_4b_1+a_2b_3-a_3b_2).$$

则 H 作成一个环. 而且四元数除环 $\bar{R}$ 与 H 同构.

$$\psi: a+bi+cj+dk \to (a,b,c,d)$$

是 $\bar{R}$ 与 H 间的一个同构映射.

4) 设

$$Q=\left\{\begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix} \,\middle|\, a,b,c,d \text{ 是实数}\right\}$$

对于矩阵的加法和乘法来说作成一个环. 则四元数除环 $\bar{R}$ 与 Q 同构.

$$\psi: a+bi+cj+dk \to \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix}$$

是 $\bar{R}$ 与 Q 间的一个同构映射.

5) 我们已经知道 5 个形式不同但结构相同的四元数除环,它是历史上第一个不可换除环,它是被英国一位数学家、物理学家汉弥尔顿(Hamilton)在 1843 年构造出来的. 汉弥尔顿原来想,复数是由实数对构造出来的,即 $\left\{(a,b)\,\middle|\,a,b \text{ 是实数}\right\}$ 是一个复数域. 那么能否把复数再扩张,使实数三元有序组的集 $\left\{(a,b,c)\,\middle|\,a,b,c \text{ 是实数}\right\}$ 成为一个域呢? 结果失败了. 后来,他构造出一个实数四元有序组的集,可以作成非交换除环,不是一个域,这就是四元数除环. 为了解决这个问题,他花了十年时间. 由于四元数除环的发现,大量的重要的代数系统,一些超复数系统被发现、发展了,而且产生了结构理论.

7. 证明:假定 R 是一个整环,那么 R 上的一元多项式环 $R[x]$ 也是一个整环.

证 已知 $R[x]$ 是一个环.

1) $\forall f(x), g(x)\in R[x]$,有 $f(x)=a_0+a_1x+\cdots+a_nx^n$, $g(x)=b_0+b_1x+\cdots+b_mx^m$,则

$$f(x)g(x)=c_0+c_1x+\cdots+c_{n+m}x^{n+m},$$

其中 $c_k=\sum\limits_{i+j=k}a_ib_j, k=0,1,\cdots,n+m$.

$$g(x)f(x)=d_0+d_1x+\cdots+d_{m+n}x^{m+n},$$

其中 $d_k=\sum\limits_{j+i=k}b_ja_i, k=0,1,\cdots,m+n$. 因 R 是交换环,故 $c_k=d_k, k=0,1,\cdots,n+m$,从而 $f(x)g(x)=g(x)f(x)$. 所以 $R[x]$ 是交换环.

2）　因 R 有单位元 1，故 $\exists\, 1=1+0x+\cdots+0x^n\in R[x]$，使得 $\forall\, f(x)\in R[x]$，有 $1f(x)=f(x)1=f(x)$. 所以 $R[x]$有单位元.

3）　$\forall\, f(x)=a_0+a_1x+\cdots+a_nx^n$，$g(x)=b_0+b_1x+\cdots+b_mx^m\in R[x]$，且 $f(x)\neq 0$，$g(x)\neq 0$，不妨设 $a_n\neq 0$，$b_m\neq 0$，因 R 无零因子，故 $a_nb_m\neq 0$. 由

$$f(x)g(x)=a_0b_0+(a_0b_1+a_1b_0)x+\cdots+a_nb_mx^{n+m},$$

又 x 是 R 上的未定元，从而 $f(x)g(x)\neq 0$. 所以 $R[x]$无零因子.（$R[x]$无零因子还可如下证明：$\forall\, f(x)=a_0+a_1x+\cdots+a_nx^n(\neq 0)\in R[x]$，$g(x)=b_0+b_1x+\cdots+b_mx^m(\neq 0)\in R[x]$. 设 a_i 是 $a_0,a_1,\cdots,a_n$ 中第一个不等于零的元，$0\leqslant i\leqslant n$；bj 是 $b_0,b_1,\cdots,b_m$ 中第一个不等于零的元，$0\leqslant j\leqslant m$，则 $a_0=a_1=\cdots=a_{i-1}=b_0=b_1=\cdots=b_{j-1}=0$. 因 R 无零因子，故 $f(x)g(x)$ 的第$i+j+1$项的系数 $a_0b_{i+j}+a_1b_{i+j-1}+\cdots+a_{i-1}b_{j+1}+a_ib_j+a_{i+1}b_{j-1}+\cdots+a_{i+j}b_0=a_ib_j\neq 0$. 又 x 是 R 上的未定元，从而 $f(x)g(x)\neq 0$.）

综上可知 $R[x]$是一个整环.

注　该命题的逆命题也成立. 即：设 R 是有单位元的交换环，则

$$R\text{ 是整环}\Leftrightarrow R[x]\text{ 是整环}.$$

证　（$\Rightarrow$）　已证.

（$\Leftarrow$）　（反证法）设 R 不是整环，则 R 有零因子，但 $R\subset R[x]$，从而 R 的零因子也是 $R[x]$的零因子，于是 $R[x]$有零因子，此与已知矛盾. 所以 R 是整环.

命题的逆否形式为：设 R 是有单位元的交换环，则

$$R\text{ 不是整环}\Leftrightarrow R[x]\text{ 不是整环}.$$

例　因 $\mathbb{Z}_6$ 是有单位元的交换环，但有零因子，故环 $\mathbb{Z}_6[x]$不是整环.

8. 假定 $\mathbb{Z}_7$ 是模 7 的剩余类环. 在 $\mathbb{Z}_7[x]$里把乘积

$$([3]x^3+[5]x-[4])([4]x^2-x+[3])$$

计算出来.

解

$$\begin{aligned}\text{原式}=&[3][4]x^5-[3]x^4+([5][4]+[3][3])x^3+(-[4][4]-[5])x^2+\\&([4]+[5][3])x-[4][3]\\=&[5]x^5+[-3]x^4+[1]x^3+[0]x^2+[5]x+[-5]\\=&[5]x^5+[4]x^4+x^3+[5]x+[2].\end{aligned}$$

9. 证明：

1）　$R[\alpha_1,\alpha_2]=R[\alpha_2,\alpha_1]$.

2）　若 $x_1,x_2,\cdots,x_n$ 是 R 上的无关未定元，那么每一个 x_i 都是 R 上的未定元.

证一　1）

$$R[\alpha_1,\alpha_2]=\left\{\sum_{i_1i_2}a_{i_1i_2}\alpha_1^{i_1}\alpha_2^{i_2}\,\middle|\,a_{i_1i_2}\in R,\text{只有有限个 }a_{i_1i_2}\neq 0\right\}.$$

$$R[\alpha_2,\alpha_1]=\left\{\sum_{j_1j_2}a_{j_2j_1}\alpha_2^{j_2}\alpha_1^{j_1}\,\middle|\,a_{j_2j_1}\in R,\text{只有有限个 }a_{j_2j_1}\neq 0\right\}.$$

$\forall\sum\limits_{i_1i_2}a_{i_1i_2}\alpha_1^{i_1}\alpha_2^{i_2}\in R[\alpha_1,\alpha_2]$，因 $\alpha_1,\alpha_2\in R_0$，而 R_0 是以 R 为子环的交换环，故

$$\sum_{i_1i_2}a_{i_1i_2}\alpha_1^{i_1}\alpha_2^{i_2}=\sum_{i_2i_1}a_{i_1i_2}\alpha_2^{i_2}\alpha_1^{i_1}\in R[\alpha_2,\alpha_1],$$

从而 $R[\alpha_1,\alpha_2]\subset R[\alpha_2,\alpha_1]$. 同理 $R[\alpha_2,\alpha_1]\subset R[\alpha_1,\alpha_2]$. 所以 $R[\alpha_1,\alpha_2]=R[\alpha_2,\alpha_1]$.

2) 设 $\sum_{k=0}^{m} a_k x_i^k = 0$, $i=1,2,\cdots,n$, $a_k\in R$, 则

$$\sum_{k=0}^{m} a_k x_1^0 \cdots x_{i-1}^0 x_i^k x_{i+1}^0 \cdots x_n^0 = 0.$$

因 $x_1,x_2,\cdots,x_i,\cdots,x_n$ 是 R 上无关未定元, 故 $a_0=a_1=\cdots=a_m=0$, 从而 x_i 是 R 上未定元.

证二 1) $\forall f(\alpha_1,\alpha_2)\in R[\alpha_1,\alpha_2]=R[\alpha_1][\alpha_2]$, 即 $f(\alpha_1,\alpha_2)$ 是环 $R[\alpha_1]$ 上 α_2 的多项式. 因 $R[\alpha_1,\alpha_2]$ 是交换环, 故 $f(\alpha_1,\alpha_2)$ 总可写成环 $R[\alpha_2]$ 上 α_1 的多项式, 从而 $f(\alpha_1,\alpha_2)\in R[\alpha_2][\alpha_1]=R[\alpha_2,\alpha_1]$, 于是 $R[\alpha_1,\alpha_2]\subset R[\alpha_2,\alpha_1]$, 同理 $R[\alpha_2,\alpha_1]\subset R[\alpha_1,\alpha_2]$. 所以 $R[\alpha_1,\alpha_2]=R[\alpha_2,\alpha_1]$.

2) (反证法)设某 x_i 不是 R 上未定元, 则必有不全为 0 的 R 中的元 $a_0,a_1\cdots,a_m$, 使得

$$a_0+a_1x_i+\cdots+a_mx_i^m=0.$$

左边可以看成 R 上无关未定元 $x_1,x_2,\cdots,x_n$ 的一个多项式, 其中 $x_1,x_2,\cdots,x_{i-1},x_{i+1},\cdots,x_n$ 的指数都取 0. 但 $a_0,a_1,\cdots,a_m$ 不全为 0, 此与 $x_1,x_2,\cdots,x_n$ 是无关未定元矛盾.

10. 证明:

1) 若 $x_1,x_2,\cdots,x_n$ 和 $y_1,y_2,\cdots,y_n$ 是 R 上的两组无关未定元, 那么

$$R[x_1,x_2,\cdots,x_n]\cong R[y_1,y_2,\cdots,y_n].$$

2) R 上的一元多项式环 $R[x]$ 能与它的一个真子环同构.

证 1)

$$\phi: f(x_1,x_2,\cdots,x_n)\to f(y_1,y_2,\cdots,y_n)$$

是 $R[x_1,x_2,\cdots,x_n]$ 到 $R[y_1,y_2,\cdots,y_n]$ 的同态满射[①]. 下面证明 ϕ 是单射. $\forall f_1(x_1,x_2,\cdots,x_n)$, $f_2(x_1,x_2,\cdots,x_n)\in R[x_1,x_2,\cdots,x_n]$, 若 $f_1(y_1,y_2,\cdots,y_n)=f_2(y_1,y_2,\cdots,y_n)$, 因 $y_1,y_2,\cdots,y_n$ 是 R 上无关未定元, 故 $f_1(y_1,y_2,\cdots,y_n)$ 与 $f_2(y_1,y_2,\cdots,y_n)$ 的系数对应相等, 即 $f_1(x_1,x_2,\cdots,x_n)$ 与 $f_2(x_1,x_2,\cdots,x_n)$ 的系数对应相等, 从而 $f_1(x_1,x_2,\cdots,x_n)=f_2(x_1,x_2,\cdots,x_n)$. 综上, ϕ 是 $R[x_1,x_2,\cdots,x_n]$ 与 $R[y_1,y_2,\cdots,y_n]$ 间的一个同构映射. 所以 $R[x_1,x_2,\cdots,x_n]\cong R[y_1,y_2,\cdots,y_n]$.

2) 令

$$R[x^2]=\left\{a_0+a_1x^2+\cdots+a_nx^{2n}\,\middle|\,a_i\in R\right\}.$$

显然 $R[x^2]\subset R[x]$. 又 $1\in R[x^2]$, 从而 $R[x^2]\neq\varnothing$. 且 $x\in R[x]$, 但 $x\overline{\in} R[x^2]$. 假设不然, $x\in R[x^2]$, 有

$$x=b_0+b_1x^2+\cdots+b_mx^{2m}.$$

即

$$b_0-x+b_1x^2+\cdots+b_mx^{2m}=0,$$

其中系数 $b_0,-1,b_1,0,b_2,0,b_3,\cdots,b_m(\in R)$ 不全为 0, 此与 x 是 R 上未定元矛盾. 于是 $x\overline{\in} R[x^2]$. 所以 $R[x^2]$ 是 $R[x]$ 的不空真子集.

因为 $R[x^2]$ 对于 R_0 的运算来说作成 R 上的多项式环, 所以由定义知, $R[x^2]$ 是 $R[x]$ 的真子环.

---

① 张禾瑞. 近世代数基础. 北京: 高等教育出版社, 1978. 108. 定理 3.

$x^2\in R_0$，设

$$c_0+c_1x^2+c_2x^4+\cdots+c_kx^{2k}=0,$$

其中 $c_i\in R$. 因 x 是 R 上未定元，故系数

$$c_0=c_1=c_2=\cdots=c_k=0.$$

所以 x^2 是 R 上未定元.

由本题 1)知，$R[x]\cong R[x^2]$. 即 $R[x]$ 与它的一个真子环 $R[x^2]$ 同构.

注 1) 设 R_0 是一个有单位元的交换环，$\alpha_1,\alpha_2,\cdots,\alpha_n$ 与 $\beta_1,\beta_2,\cdots,\beta_n$ 都是 R_0 中的任意元，R 是包含 R_0 的单位元的 R_0 的子环. 则

$$\phi: f(\alpha_1,\alpha_2,\cdots,\alpha_n)\to f(\beta_1,\beta_2,\cdots,\beta_n)$$

未必是 $R[\alpha_1,\alpha_2,\cdots,\alpha_n]$ 到 $R[\beta_1,\beta_2,\cdots,\beta_n]$ 的映射.

例 取 $\alpha\in R$ ，$\beta\in R_0$，$\alpha\neq\beta$. 对于 $f(\alpha)=0\in R[\alpha]$，有

$$\phi: f(\alpha)=0=\alpha+(-1)\alpha\to\alpha+(-1)\beta=\alpha-\beta,$$

$$f(\alpha)=0=0+0\alpha\to 0+0\beta=0.$$

因 $\alpha-\beta\neq0$，故 $f(\alpha)=0$ 的象不唯一，从而ϕ不是映射.

2) 设 $x_1,x_2,\cdots,x_n$ 是 R 上无关未定元，$\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 R_0 中的任意 n 个元. 则

$$\phi: f(x_1,x_2,\cdots,x_n)\to f(\alpha_1,\alpha_2,\cdots,\alpha_n)$$

是 $R[x_1,x_2,\cdots,x_n]$ 到 $R[\alpha_1,\alpha_2,\cdots,\alpha_n]$ 的同态满射. 由此知：在 $R[x_1,x_2,\cdots,x_n]$ 中，若

$$h(x_1,x_2,\cdots,x_n)=f(x_1,x_2,\cdots,x_n)+g(x_1,x_2,\cdots,x_n),$$

$$k(x_1,x_2,\cdots,x_n)=f(x_1,x_2,\cdots,x_n)g(x_1,x_2,\cdots,x_n),$$

则在 $R[\alpha_1,\alpha_2,\cdots,\alpha_n]$ 中，有

$$h(\alpha_1,\alpha_2,\cdots,\alpha_n)=f(\alpha_1,\alpha_2,\cdots,\alpha_n)+g(\alpha_1,\alpha_2,\cdots,\alpha_n),$$

$$k(\alpha_1,\alpha_2,\cdots,\alpha_n)=f(\alpha_1,\alpha_2,\cdots,\alpha_n)g(\alpha_1,\alpha_2,\cdots,\alpha_n),$$

从而保证了《高等代数》[①]中，将多项式中的 x 代值的合理性. 例，证明余式定理时，设 $f(x)=(x-\alpha)g(x)+r$，$r=0$ 或 $\deg r=0$，有 $f(\alpha)=(\alpha-\alpha)g(\alpha)+r=r$. 把 x 用α 代换后，仍保持原来的运算关系.

ϕ还满足：$\phi(x_i)=\alpha_i$，$i=1,2,\cdots,n$. $\phi(a)=a$，$\forall a\in R$.

但要注意ϕ可能不是单射. 因为 $f(\alpha_1,\alpha_2,\cdots,\alpha_n)(\in R[\alpha_1,\alpha_2,\cdots,\alpha_n])$ 的表法可能不唯一，所以 $f(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 在ϕ下的逆象就可能不唯一. 例，设 x 是 R 上无关未定元，$\alpha\in R$，取 $f(\alpha)=0\in R[\alpha]$. 因 $f(\alpha)=0+0\alpha$，故 $\exists\, 0+0x\in R[x]$，使得$\phi(0+0x)=f(\alpha)$，又因 $f(\alpha)=\alpha+(-1)\alpha$，故 $\exists\,\alpha+(-1)x\in R[x]$，使得$\phi(\alpha+(-1)x)=f(\alpha)$，但 $0+0x\neq\alpha+(-1)x$. 所以ϕ不是 $R[x]$ 到 $R[\alpha]$ 的单射. 又例，π是 $\mathbb{Z}$ 上未定元，$\mathbb{Z}[\pi]\overset{\phi}{\sim}\mathbb{Z}[\sqrt{2}]$，$\phi$：$f(\pi)\to f(\sqrt{2})$，从而$\phi$：$3\pi\to3\sqrt{2}$，$\pi+\pi^3\to\sqrt{2}+(\sqrt{2})^3=3\sqrt{2}$. 但 $3\pi\neq\pi+\pi^3$. 所以ϕ不是 $\mathbb{Z}[\pi]$ 到 $\mathbb{Z}[\sqrt{2}]$ 的单射.

3) 由本题 1)知，有单位元的交换环 R 上的 n 个无关未定元的多项式环在同构意义下是唯一的.

4) 仿本题证明 x^2 是 R 上未定元的方法，可证：若 x 是 R 上未定元，则 $x^k(k\geqslant1)$ 也是 R 上的未定元. 还可用反证法证明如下：假设 x^k 不是 R 上未定元，则 $\exists$ 不全为 0 的元

---

① 北京大学数学系几何与代数教研室. 高等代数. 北京：高等教育出版社，1978

$a_0, a_1, \cdots, a_m \in R$，使得 $a_0 + a_1 x^k + \cdots + a_m (x^k)^m = 0$，即

$$a_0 + a_1 x^k + \cdots + a_m x^{km} = 0.$$

因 $a_0, a_1, \cdots, a_m$ 不全为 0，故 x 不是 R 上未定元，此与题设矛盾. 所以 x^k 是 R 上未定元.

当 $k \geqslant 1$ 时，$R[x^k]$ 也是 $R[x]$ 的真子环且 $R[x] \cong R[x^k]$. 即 $R[x]$ 能与它的无穷多个真子环同构.

5) 由本题 2)知，无限环可能与其某个真子环同构.

三、讲与练

1. 设ϕ是环 R 到环 $\bar{R}$ 的同态满射. 在以下各命题中，如正确则给出证明，不正确则举出反例.

1) $\forall a, b \in R$，有$\phi(a-b) = \phi(a) - \phi(b)$.

2) $\forall a \in R, n \in \mathbb{Z}$，有$\phi(na) = n\phi(a)$.

3) 若 $\bar{R}$ 是交换环，则 R 也是交换环.

4) 若 $\bar{R}$ 有单位元，则 R 也有单位元.

5) 若 R 有单位元，$a \in R$，a 有逆元 a^{-1}，则$\phi(a)$有逆元$[\phi(a)]^{-1}$，且$[\phi(a)]^{-1} = \phi(a^{-1})$.

6) 若 R 与 $\bar{R}$ 都有单位元，$\bar{a} \in \bar{R}$，$\bar{a}$ 有逆元$\bar{a}^{-1}$，则 $\bar{a}$ 的逆象 a 也有逆元 a^{-1}，且 a^{-1} 是 $\bar{a}^{-1}$ 的逆象.

7) 若 R 与 $\bar{R}$ 都有单位元，$\forall n \in \mathbb{Z}$，$a \in R$，且 a 有逆元 a^{-1}，则$\phi(a^n) = [\phi(a)]^n$.

8) 若 R 无零因子，则 $\bar{R}$ 无零因子.

9) 若 $\bar{R}$ 无零因子，则 R 无零因子.

10) 若 R 是整环，则 $\bar{R}$ 是整环.

11) 若 $\bar{R}$ 是整环，则 R 是整环.

12) 若 R 是除环，则 $\bar{R}$ 是除环.

13) 若 $\bar{R}$ 是除环，则 R 是除环.

14) 若 R 是域，则 $\bar{R}$ 是域.

15) 若 $\bar{R}$ 是域，则 R 是域.

16) 若 $a \in R$，a 是 R 的幂等元，则$\phi(a)$是 $\bar{R}$ 的幂等元.

17) 若 $a \in R$，a 是 R 的幂零元，则$\phi(a)$是 $\bar{R}$ 的幂零元.

解 1) 正确. 事实上，

$$\phi(a-b) = \phi[a+(-b)] = \phi(a) + \phi(-b) = \phi(a) + [-\phi(b)] = \phi(a) - \phi(b).$$

2) 正确. 事实上，当 $n > 0$ 时，有

$$\phi(na) = \phi(\overbrace{a + a + \cdots + a}^{n\text{个}}) = \overbrace{\phi(a) + \phi(a) + \cdots + \phi(a)}^{n\text{个}} = n\phi(a);$$

当 $n = 0$ 时，有

$$\phi(na) = \phi(0) = 0 = n\phi(a);$$

当 $n < 0$ 时，$-n > 0$，有

$$\phi(na) = \phi[-(-na)] = -\phi[(-n)a] = -(-n)\phi(a) = n\phi(a).$$

所以 $\forall n \in \mathbb{Z}$，有$\phi(na) = n\phi(a)$.

3)　不正确. 例,$\phi:\begin{pmatrix} a_1 & a_2 \\ 0 & 0 \end{pmatrix} \to a_1$ 是环 $R=\left\{\begin{pmatrix} a_1 & a_2 \\ 0 & 0 \end{pmatrix} \middle| a_i \in \mathbb{R}\right\}$ 到环 $\bar{R}=\mathbb{R}$ 的一个同态满射. $\bar{R}$ 是交换环,但 $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$,从而 R 不是交换环. 又例,$\phi:\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to 0$ 是环 $R=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d \in \mathbb{R}\right\}$ 到环 $\bar{R}=\{0\}$ 的一个同态满射. $\bar{R}$ 是交换环,但 R 为非交换环.

4)　不正确. 例,$\phi:2n\to 0$ 是环 $R=2\mathbb{Z}=\{2n \mid n\in\mathbb{Z}\}$ 到环 $\bar{R}=\{0\}$ 的一个同态满射. $\bar{R}$ 有单位元 0,但 R 无单位元. 由本题 3)中第一个例子也可知 4)不成立(见第九章,三,1,1)).

5)　正确. 事实上,因为

$$\phi(a)\,\phi(a^{-1}) = \phi(aa^{-1}) = \phi(1),\ \phi(a^{-1})\,\phi(a) = \phi(a^{-1}a) = \phi(1),$$

又 $\phi(1)$ 是 $\bar{R}$ 的单位元,所以 $[\phi(a)]^{-1}=\phi(a^{-1})$.

6)　不正确. 例,设 $R=\mathbb{Z}_6$,$\bar{R}=\mathbb{Z}_3$ 都有单位元. $\phi:[0]\to[0],[1]\to[1],[2]\to[2],[3]\to[0],[4]\to[1],[5]\to[2]$ 是 $\mathbb{Z}_6$ 到 $\mathbb{Z}_3$ 的同态满射. $[2]\in\mathbb{Z}_3$,$[2]$ 有逆元,但 $[2]$ 的逆象 $[2](\in\mathbb{Z}_6)$ 是 $\mathbb{Z}_6$ 的零因子(因 $[2][3]=[0]$),由第九章,三,1,3),①知,$[2](\in\mathbb{Z}_6)$ 没有逆元.

7)　正确. 事实上,当 $n>0$ 时,有

$$\phi(a^n) = \phi(\overbrace{a\ \ a\ \ \cdots\ \ a}^{n\text{个}}) = \overbrace{\phi(a)\,\phi(a)\,\cdots\,\phi(a)}^{n\text{个}} = [\phi(a)]^n.$$

当 $n=0$ 时,因 $a^0=1$,$\phi(1)$ 是 $\bar{R}$ 的单位元,故

$$\phi(a^n) = \phi(a^0) = \phi(1) = [\phi(a)]^0 = [\phi(a)]^n;$$

当 $n<0$ 时,$-n>0$,由 a 有逆元 a^{-1} 及本题 5),有

$$\phi(a^n) = \phi[(a^{-1})^{-n}] = [\phi(a^{-1})]^{-n} = [(\phi(a))^{-1}]^{-n} = [\phi(a)]^n.$$

所以 $\forall n\in\mathbb{Z}$,有 $\phi(a^n)=[\phi(a)]^n$.

8)　不正确①.

9)　不正确. 例,$\phi:\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \to \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ 是环 $R=\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a,b,c\in\mathbb{R}\right\}$ 到环 $\bar{R}=\left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| a\in\mathbb{R}\right\}$ 的一个同态满射. $\bar{R}$ 无零因子,但 R 有零因子. 因 $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. 又例,由本题 6)知,$\mathbb{Z}_6\sim\mathbb{Z}_3$,$\mathbb{Z}_3$ 无零因子,但 $\mathbb{Z}_6$ 有零因子.

10)　不正确. 例,$\mathbb{Z}\sim\mathbb{Z}_4$,$\mathbb{Z}$ 是整环,但 $\mathbb{Z}_4$ 有零因子,从而 $\mathbb{Z}_4$ 不是整环.

11)　不正确. 见本题 9)中的例,$\bar{R}$ 是整环,而 R 不是整环.

12)　不正确. 例,$\phi:x\to 0$ 是有理数环 $\mathbb{Q}$ 到零环 $\{0\}$ 的同态满射. $\mathbb{Q}$ 是除环,但 $\{0\}$ 不是除环.

若环 $R \overset{\phi}{\sim}$ 环 $\bar{R}$,R 是除环且 $\bar{R}$ 至少包含一个不等于零的元,则 $\bar{R}$ 是除环. 事实上,因除环 R 有单位元 1,故 $\bar{R}$ 有单位元 $\phi(1)$. $\forall \bar{a}\in\bar{R}$,$\bar{a}\neq\bar{0}$,其中 $\bar{0}$ 是 $\bar{R}$ 的零元,因 ϕ 是满射,故 $\exists\, a(\neq 0)\in R$,使得 $\phi(a)=\bar{a}$. 因 R 是除环,故 $\exists\ a^{-1}\in R$,由本题 5),$\bar{a}=\phi(a)$ 有逆元 $\bar{a}^{-1}=$

① 张禾瑞. 近世代数基础. 北京:高等教育出版社,1978. 98. 例 3.

$\phi(a^{-1})\in\bar{R}$，所以 $\bar{R}$ 是除环.（还可如下证明：因 R 是除环，故 $R^*=R-\{0\}$ 作成乘群. 因 $R\sim\bar{R}$，故 $R^*\sim\bar{R}^*=\bar{R}-\{\bar{0}\}$，其中 $\bar{0}$ 是 $\bar{R}$ 的零元. 于是 $\bar{R}^*$ 是一个乘群. 从而 $\bar{R}$ 是一个除环.）

13） 不正确. 例，取 $R=\mathbb{Z}$，$\bar{R}=\mathbb{Z}_p$，其中 p 是素数. $\phi:a\to[a]$ 是 $\mathbb{Z}$ 到 $\mathbb{Z}_p$ 的一个同态满射. $\mathbb{Z}_p$ 是除环，而 $\mathbb{Z}$ 不是除环. 又例，取 $R=2\mathbb{Z}=\left\{2n\,\middle|\,n\in\mathbb{Z}\right\}$，$\bar{R}=\mathbb{Z}_2$. $\forall n\in\mathbb{Z}$，

$$\phi:4n\to[0],\ 4n-2\to[1]$$

是 $2\mathbb{Z}$ 到 $\mathbb{Z}_2$ 的一个同态满射. $\mathbb{Z}_2$ 是除环，但 $2\mathbb{Z}$ 不是除环. 又例，$R=\left\{(a,b)\,\middle|\,a,b\in\mathbb{Q}\right\}$ 对于

$$(a_1,b_1)=(a_2,b_2)\Leftrightarrow a_1=a_2,b_1=b_2,$$

$$(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_2),$$

$$(a_1,b_1)(a_2,b_2)=(a_1a_2,b_1b_2)$$

作成一个环，因 R 有零因子，故 R 不是除环. $\phi:(a,b)\to a$ 是 R 到有理数环 $\mathbb{Q}$ 的一个同态满射，而 $\mathbb{Q}$ 是除环.

14） 不正确. 例见本题 12）.

若环 $R\sim$ 环 $\bar{R}$，R 是域而 $\bar{R}$ 至少有两个元，则 $\bar{R}$ 是域. 证明与本题 12）类似.

15） 不正确. 例见本题 13）. 又例，

$$\phi:f(x)=a_0+a_1x+\cdots+a_nx^n\to f(0)=a_0$$

是环 $\mathbb{R}[x]$ 到环 $\mathbb{R}$ 的一个同态满射. $\mathbb{R}$ 是域，但 $\mathbb{R}[x]$ 不是域，因 $x(\in\mathbb{R}[x])$ 无逆元. 又例，

$$\phi:[0]\to[0],\ [1]\to[1],\ [2]\to[0],\ [3]\to[1]$$

是环 $\mathbb{Z}_4$ 到环 $\mathbb{Z}_2$ 的一个同态满射. $\mathbb{Z}_2$ 是域，但 $\mathbb{Z}_4$ 不是域.

16） 正确. 事实上，因 a 是 R 的幂等元，由第九章，四，12 知，$a^2=a$. 从而由本题 7）有

$$[\phi(a)]^2=\phi(a^2)=\phi(a).$$

所以 $\phi(a)$ 是 $\bar{R}$ 的幂等元.

17） 正确. 事实上，因 a 是 R 的幂零元，由第九章，四，12 知，$\exists$ 正整数 n，使得 $a^n=0$，从而

$$[\phi(a)]^n=\phi(a^n)=\phi(0)=0.$$

所以 $\phi(a)$ 是 $\bar{R}$ 的幂零元.

2. 设环 $R\overset{\phi}{\cong}$ 环 $\bar{R}$，证明：

1） R 的零因子在 ϕ 下的象是 $\bar{R}$ 的零因子.

2） $\bar{R}$ 的零因子在 ϕ 下的逆象是 R 的零因子.

证 1） 设 $a(\in R)$ 是 R 的零因子，则 $a\neq0$，且 $\exists\ b\ (\neq0)\in R$，使得 $ab=0$. 设 $\phi(a)=\bar{a}$，$\phi(b)=\bar{b}$，则 $\phi(ab)=\phi(a)\phi(b)=\bar{a}\,\bar{b}$. 今 $ab=0$，从而 $\bar{a}\,\bar{b}=\bar{0}$，其中 $\bar{0}$ 是 $\bar{R}$ 的零元. 因 $a\neq0$，$b\neq0$，又 ϕ 是单射，故 $\bar{a}\neq\bar{0}$，$\bar{b}\neq\bar{0}$. 于是 $\bar{a}$ 是 $\bar{R}$ 的左零因子. 同理可证 $\bar{a}$ 是 $\bar{R}$ 的右零因子. 所以 a 在 ϕ 下的象 $\bar{a}$ 是 $\bar{R}$ 的零因子.

2） 设 $\bar{a}(\in\bar{R})$ 是 $\bar{R}$ 的零因子，则 $\bar{a}\neq\bar{0}$ 且 $\exists\ \bar{b}\ (\neq\bar{0})\in\bar{R}$，使得 $\bar{a}\,\bar{b}=\bar{0}$. 因 ϕ 是满射，故 $\exists\,a,b\in R$，使得 $\phi(a)=\bar{a}$，$\phi(b)=\bar{b}$，从而 $\phi(ab)=\phi(a)\phi(b)=\bar{a}\,\bar{b}=\bar{0}$. 因 ϕ 是单射，故 $ab=0$. 因 $\bar{a}\neq\bar{0}$，$\bar{b}\neq\bar{0}$，故 $a\neq0$，$b\neq0$. 于是 a 是 R 的左零因子. 同理可证 a 是 R 的右零因子. 所以 $\bar{a}$ 在 ϕ 下的逆象 a 是 R 的零因子.

注 1） 由该命题知：设环 $R\cong$ 环 $\bar{R}$，则

$$R\text{ 有零因子}\Leftrightarrow\bar{R}\text{ 有零因子},$$

即

$$R\text{ 无零因子}\Leftrightarrow \bar{R}\text{ 无零因子}.$$

2）　同构的两个环实际上是一个环的两种不同的表现形式，是一个环的两个样品，它们的代数性质完全一样．所谓代数性质，就是从环的定义出发，经过逻辑推理得到的性质．近世代数是研究代数系统的那些在同构映射下仍保持不变的性质．

3）　环 $R=\left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a,b\in \mathbb{Z}\right\}$ 与数环 $\bar{R}$（元是数，代数运算是普通数的加法与乘法）不同构．因 R 有零因子，$\bar{R}$ 无零因子，故由该命题知，R 与 $\bar{R}$ 不同构．

3. 设 ϕ 是环 R 到环 $\bar{R}$ 的一个同态映射．判断以下各命题是否正确．

1）　$\phi(0)=\bar{0}$，其中 0 与 $\bar{0}$ 分别是 R 与 $\bar{R}$ 的零元．

2）　$\forall\ a\in R,\phi(-a)=-\phi(a)$．

3）　若 R 是交换环，则 $\bar{R}$ 也是交换环．

4）　若 R 有单位元，则 $\bar{R}$ 也有单位元．

5）　若 R 与 $\bar{R}$ 都有单位元，$a\in R$，a 有逆元，则 $\phi(a)$ 也有逆元．

解　1）　正确．事实上，因 $\phi(0)=\phi(0+0)=\phi(0)+\phi(0)$，故 $\phi(0)=\phi(0)-\phi(0)=\bar{0}$（见第五章，一，2，1））．

2）　正确．事实上，$\phi(a)+\phi(-a)=\phi[a+(-a)]=\phi(0)=\bar{0}$，从而 $\phi(-a)=-\phi(a)$（见第五章，一，2，2））．

3）　不正确．例，$\phi:a\to\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ 是整数环 $\mathbb{Z}$ 到矩阵环 $M=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d\in \mathbb{Z}\right\}$ 的同态映射．$\mathbb{Z}$ 是交换环，M 不是交换环．

4）　不正确．例，设 R 是有理数环．$\bar{R}=\{0,x\}$ 对于

$+$	0	x
0	0	x
x	x	0

$\cdot$	0	x
0	0	0
x	0	0

来说作成一个环．$\phi:a\to 0$ 是 R 到 $\bar{R}$ 的一个同态映射．R 有单位元 1，$\bar{R}$ 无单位元．

5）　不正确．例，$\phi:a\to[0]$ 是实数环 $\mathbf{R}$ 到模 2 的剩余类环 $\mathbb{Z}_2$ 的一个同态映射．$\mathbf{R}$ 有单位元 1，$\mathbb{Z}_2$ 有单位元 $[1]$．$3(\in\mathbf{R})$ 有逆元 $\frac{1}{3}\in\mathbf{R}$，但 $\phi(3)=[0]$ 无逆元．

4. 证明：整数环 $\mathbb{Z}$ 与偶数环 $2\mathbb{Z}$ 不同构．

证　因 $\mathbb{Z}$ 有单位元 1，而 $2\mathbb{Z}$ 无单位元，故知 $\mathbb{Z}$ 与 $2\mathbb{Z}$ 不同态①，当然 $\mathbb{Z}$ 与 $2\mathbb{Z}$ 也不同构．

注　1）　$\phi:n\to 2n$ 是整数加群与偶数加群间的同构映射，从而整数加群与偶数加群同构．但整数环与偶数环不同构．说明环的同构必需是对于两对代数运算来说的．

2）　设 $\mathbb{Z}$ 是整数集，若规定：$\forall\ a,b\in\mathbb{Z}$，

$$a\oplus b=a+b,\ a\odot b=2ab.$$

① 张禾瑞．近世代数基础．北京：高等教育出版社，1978．98．定理 2．

则 $\mathbb{Z}$ 对于 $\oplus$, $\odot$ 来说作成一个环. 此时, ϕ : $a \to 2a$ 是环 $\mathbb{Z}$ 与偶数环 $2\mathbb{Z}$ 间的一个同构映射. 不过要注意,这里环 $\mathbb{Z}$ 的代数运算不是普通数的运算.

3) 设 $2\mathbb{Z}$ 是偶数集,若规定 : $\forall 2n, 2m \in 2\mathbb{Z}$,

$$2n \oplus 2m = 2(n+m) \text{ , } 2n \odot 2m = \frac{2n \cdot 2m}{2} = 2nm.$$

则 $2\mathbb{Z}$ 对于 $\oplus$, $\odot$ 来说作成一个环. 此时 , ϕ: $n \to 2n$ 是整数环 $\mathbb{Z}$ 与环 $2\mathbb{Z}$ 间的一个同构映射. 如果将环 $2\mathbb{Z}$ 的代数运算改成普通数的运算,那么 $\mathbb{Z}$ 与 $2\mathbb{Z}$ 就不同构了. 因此同构与否,与代数运算关系密切.

5. 设 ϕ 是域 F 到域 $\overline{F}$ 的一个同态满射,证明: ϕ 是 F 到 $\overline{F}$ 的一个单射. 从而 $F \overset{\phi}{\cong} \overline{F}$.

证 (反证法) $\forall a, b \in F, a \neq b$. 设 $\phi(a) = \bar{a}, \phi(b) = \bar{b}$. 若 $\bar{a} = \bar{b}$,则由第十一章,三,1,1),

$$\phi(a-b) = \phi(a) - \phi(b) = \bar{a} - \bar{b} = \bar{0},$$

其中 $\bar{0}$ 是域 $\overline{F}$ 的零元. 但 $a-b(\neq 0) \in F$,从而 $\exists (a-b)^{-1} \in F$ 且由第十一章,三,1,5),

$$\phi[(a-b)^{-1}] = [\phi(a-b)]^{-1} = \bar{0}^{-1} \in \overline{F},$$

此与域 $\overline{F}$ 的零元 $\bar{0}$ 无逆元矛盾. 从而 $\bar{a} \neq \bar{b}$. 所以 ϕ 是单射.

注 1) 在环到环的同态满射下,非零元的象未必是非零元. 但在域到域的同态满射下,非零元的象必为非零元.

2) 见后面第十二章,一,4,20).

6. 我们给出**引理** 假定在集合 A 与 $\overline{A}$ 之间存在一个一一映射 ϕ,并且 A 有加法和乘法. 那么我们可以替 $\overline{A}$ 规定加法和乘法,使得 A 与 $\overline{A}$ 对于一对加法以及一对乘法来说都同构.

证明 假定在给定的一一映射之下, A 的元 x 同 $\overline{A}$ 的元 $\bar{x}$ 对应. 我们规定:

$$\bar{a} + \bar{b} = \bar{c}, \text{若 } a + b = c,$$
$$\bar{a}\,\bar{b} = \bar{d}, \text{若 } ab = d.$$

这样规定的法则是 $\overline{A}$ 的加法和乘法,因为给了 $\bar{a}$ 和 $\bar{b}$,我们可以找到唯一的 a 和 b,因而找到唯一的 c 和 d,唯一的 $\bar{c}$ 和 $\bar{d}$.

这样规定以后, ϕ 显然对于一对加法和一对乘法来说都是同构映射. 证完.

该引理有何意义? 证明的关键之处为何?

解 引理不仅为挖补定理(或嵌入定理)提供了理论依据,而且本身也有它的重要性. 引理实质上说明了任意两个集合 A 与 $\overline{A}$ 间的一一映射 ϕ 总可以成为同构映射. 比如 A 的元素比较复杂,不便研究,那么我们可以把 A 过渡到 $\overline{A}$,掌握了 $\overline{A}$ 的构造,当然也就掌握了 A 的构造.

证明的关键是恰当地规定 $\overline{A}$ 的代数运算 $\bar{\circ}$. 设 A 的代数运算是 $\circ$. $\forall \bar{a}, \bar{b} \in \overline{A}$,把 $\bar{a}, \bar{b}$ 在 ϕ 下的逆象 a, b 的运算结果 $a \circ b = c (\in A)$ 在 ϕ 下的象 $\bar{a} \,\bar{\circ}\, \bar{b} = \bar{c}$ 规定为 $\bar{a} \,\bar{\circ}\, \bar{b}$,即 $\bar{a} \,\bar{\circ}\, \bar{b} = \bar{c} = \bar{a} \,\bar{\circ}\, \bar{b}$.

7. 挖补定理内容如下:设

1) S 是环 R 的子环, $\overline{S}$ 是环;

2) $S \overset{\phi}{\cong} \overline{S}$;

3) S 在 R 中的补集 $R - S$ 与 $\overline{S}$ 无公共元,则 $\exists$ 环 $\overline{R}$,使得 $R \cong \overline{R}$ 且 $\overline{S}$ 是 $\overline{R}$ 的子环.

① 试叙述证明的基本思路.

② 详细证明 $\bar{S}$ 是 $\bar{R}$ 的子环.

③ 定理的作用为何?

解 ① (i) 设 $S=\{a_S,b_S,\cdots\},\bar{S}=\{\bar{a}_S,\bar{b}_S,\cdots\},\phi:x_S\to\bar{x}_S$.

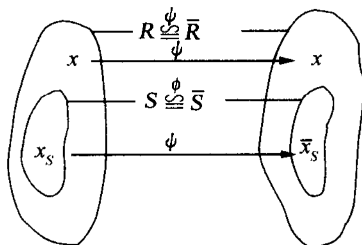
$$R=\{a_S,b_S,\cdots\in S;a,b,\cdots\in R-S\}.$$

造集

$$\bar{R}=\{\bar{a}_S,\bar{b}_S,\cdots\in\bar{S};a,b,\cdots\in R-S\}.$$

(即从 R 中把 S 挖出来,再把 $\bar{S}$ 补进去,得集 $\bar{R}$. 由已知条件 3)知,集 $\bar{R}$ 中两部分元不会有相同的.)

(ii) $\forall\ x\in R$,规定:若 $x\in S\subset R$,



$$\psi:\ x\to\bar{x}=\phi(x)=\psi(x).$$

若 $x\in R-S\subset R$,

$$\psi:x\to x=\psi(x).$$

则 ψ 是 R 与 $\bar{R}$ 间的一个一一映射. 由上面 6 中的引理,可在 $\bar{R}$ 中规定加法和乘法,使 $R\overset{\psi}{\cong}\bar{R}$. 从而 $\bar{R}$ 也是环.

(iii) $\bar{S}$ 是 $\bar{R}$ 的子环.

② 由 $\bar{R}$ 的作法,知 $\bar{S}\subset\bar{R}$. $\bar{R}$ 是环,设其代数运算为 $\bar{+}$, $\bar{\cdot}$. $\bar{S}$ 是环,设其代数运算为 $\oplus,\odot$. 设 R 的代数运算为 $+$, $\cdot$,当然 R 的子环 S 的代数运算也是 $+$, $\cdot$.

要证 $\bar{S}$ 是 $\bar{R}$ 的子环,只需证明: $\forall\bar{x},\bar{y}\in\bar{S}$,

$$\bar{x}\oplus\bar{y}=\bar{x}\bar{+}\bar{y}\quad,\quad\bar{x}\odot\bar{y}=\bar{x}\bar{\cdot}\bar{y}.$$

这样,$\bar{R}$ 的代数运算 $\bar{+}$, $\bar{\cdot}$ 施行到 $\bar{S}$ 中的元,与 $\bar{S}$ 的代数运算 $\oplus,\odot$ 的效果是相同的. 因此,由 $\bar{S}$ 对于 $\oplus$, $\odot$ 来说作成一个环,可知 $\bar{S}$ 对于 $\bar{R}$ 的代数运算 $\bar{+}$, $\bar{\cdot}$ 来说同样作成一个环,于是就证明了 $\bar{S}$ 是 $\bar{R}$ 的子环.

事实上,$\forall\ \bar{x}$, $\bar{y}\in\bar{S}$, $\exists\,x,y\in S$,使得

$$x\to\bar{x}=\phi(x)=\psi(x),$$

$$y\to\bar{y}=\phi(y)=\psi(y).$$

因 ϕ 是 S 与 $\bar{S}$ 间的同构映射,故

$$\phi:x+y=z\to\bar{x}\oplus\bar{y}.$$

因 ψ 是 R 与 $\bar{R}$ 间的同构映射,故

$$\psi:x+y=z\to\bar{x}\bar{+}\bar{y}.$$

因 $z\in S$,故 $\phi(z)=\psi(z)$. 所以 $\bar{x}\oplus\bar{y}=\bar{x}\bar{+}\bar{y}$. 同理可证 $\bar{x}\odot\bar{y}=\bar{x}\bar{\cdot}\bar{y}$. 于是 $\bar{R}$ 的加法和乘法与 $\bar{S}$ 原来已有的加法和乘法,对 $\bar{S}$ 的元的作用是相同的. 说得再详细具体一些,即: $\forall\ \bar{x},\bar{y}\in\bar{S}$,有 $\bar{x}\bar{+}\bar{y}=\bar{x}\oplus\bar{y}\in\bar{S}$, $\bar{x}\bar{\cdot}\bar{y}=\bar{x}\odot\bar{y}\in\bar{S}$,又设 $\bar{x}$ 在 $\bar{R}$ 中的负元为 $\bar{u}$,$\bar{x}$ 在 $\bar{S}$ 中的负元为 $\bar{v}$,而 $\bar{S}$ 的零元 $\bar{0}$ 就是 $\bar{R}$ 的零元,从而

$$\bar{x}\bar{+}\bar{u}=\bar{0}\quad,\quad\bar{x}\oplus\bar{v}=\bar{x}\bar{+}\bar{v}=\bar{0}.$$

于是 $\bar{x}\bar{+}\bar{u}=\bar{x}\bar{+}\bar{v}$,由 $\bar{R}$ 中加法适合消去律,$\bar{x}$ 在 $\bar{R}$ 中的负元 $\bar{u}=\bar{v}\in\bar{S}$. 依子环的判别条件知 $\bar{S}$ 是 $\bar{R}$ 的子环.

③ 挖补定理在理论和实用上都很重要. 证明未定元的存在性[①], 证明商域的存在性[②], 证明单代数扩域的存在性[③]都要用到挖补定理. 在其他的一些代数系统如群, 域中, 挖补定理仍成立.

利用挖补定理可以知道, 四元数除环由复数扩张而得, 有理数环由整数扩张而得, 整数环由自然数扩张而得. 在初等代数中对这一问题, 从逻辑上是说不清楚的, 不严密的. 而利用挖补定理, 虽然抽象一些, 但是逻辑关系是清楚的. 下面我们来看有理数环

$$R=\left\{\frac{n}{m}\,\middle|\, m,n\text{ 是整数}, m\neq 0\right\}$$

是如何由整数环 $\bar{S}=\left\{n\,\middle|\,n\text{ 是整数}\right\}$ 扩张而得.

设 $S=\left\{\frac{n}{1}\,\middle|\,n\text{ 是整数}\right\}$, 易证 S 是 R 的子环, 且 $\phi: \frac{n}{1}\to n$ 是 S 与 $\bar{S}$ 间的一个同构映射. $R-S$ 与 $\bar{S}$ 无公共元. 由挖补定理, ∃环

$$\bar{R}=\left\{n\in\bar{S}; \frac{n}{m}\in R-S\right\}.$$

$R\cong\bar{R}$ 且 $\bar{S}$ 是 $\bar{R}$ 的子环. 从而有理数环 R 由整数环 $\bar{S}$ 扩张而得.

一般来说, 利用挖补定理, 可造一个新环 $\bar{R}$, 使 $\bar{R}$ 包含一个给定的环 $\bar{S}$, 或说 $\bar{S}$ 可以扩张为新环 $\bar{R}$. 比如环 $\bar{S}$ 无单位元, 研究起来不方便, 造一个有单位元的环 $\bar{R}\supset\bar{S}$, 即把 $\bar{S}$ 嵌入到 $\bar{R}$ 中, 研究清楚 $\bar{R}$, 对 $\bar{S}$ 也就便于掌握了.

例 设 $\bar{S}$ 是一个无单位元的环, 作

$$R=\bar{S}\times\mathbb{Z}=\left\{(a,n)\,\middle|\,a\in\bar{S}, n\in\mathbb{Z}\right\}.$$

规定

$$(a,n)=(b,m)\Leftrightarrow a=b\ ,\ n=m,$$
$$(a,n)+(b,m)=(a+b\ ,\ n+m),$$
$$(a,n)(b,m)=(ab+ma+nb\ ,\ nm).$$

可验证 R 作成一个环且有单位元 $(0,1)$. $S=\left\{(a,0)\,\middle|\,a\in\bar{S}, 0\in\mathbb{Z}\right\}$ 是 R 的一个子环. $\forall (a,0)\in S$, $\phi:(a,0)\to a$ 是 S 与 $\bar{S}$ 间的一个同构映射, 即 $S\overset{\phi}{\cong}\bar{S}$. $R-S$ 与 $\bar{S}$ 无公共元. 由挖补定理, ∃环 $\bar{R}=\{x\in\bar{S}\ ;\ (a,n)\in R-S\}$, 使得 $R\cong\bar{R}$ 且 $\bar{S}$ 是 $\bar{R}$ 的子环. 因 R 有单位元 $(0,1)$, 故 $\bar{R}$ 也有单位元 $(0,1)$. 所以就把一个无单位元的环 $\bar{S}$ 嵌入到有单位元的环 $\bar{R}$ 中, 即任一无单位元的环可以看成为有单位元的子环.

由此例还可知, 整数环 $\mathbb{Z}$ 可同构嵌入到一个环 $\bar{R}'$ 中. 事实上, 若取 $S'=\left\{(0,n)\,\middle|\,0\in\bar{S}, n\in\mathbb{Z}\right\}$, 则 S' 是 R 的一个子环. $\forall (0,n)\in S'$, $\phi':(0,n)\to n$ 是 S' 与 $\mathbb{Z}$ 间的一个同构映射, 即 $S'\overset{\phi'}{\cong}\mathbb{Z}$. $R-S'$ 与 $\mathbb{Z}$ 无公共元. 由挖补定理, ∃环 $\bar{R}'=\{x\in\mathbb{Z}; (a,n)\in R-S'\}$, 使得 $R\cong\bar{R}'$ 且 $\mathbb{Z}$ 是 $\bar{R}'$ 的子环.

注 1) 任何环 R 可同构嵌入于 R 上 n 阶全矩阵环 $M_n(R)$ (见第九章, 三, 7) 中.

---

① 张禾瑞. 近世代数基础. 北京: 高等教育出版社, 1978. 103. 定理 1.

② 同上. 119. 定理 1.

③ 同上. 158. 定理 3.

2)　任意环 R 可同构嵌入于非空集 M 上的取值在环 R 内的所有函数作成的全函数环 $R\{x\}$（见第九章，三，9，注 3））中.

事实上，(i)　$S=\left\{\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a\end{pmatrix} \middle| a\in R,\text{矩阵的主对角线外的元素都是 } 0.\right\}$是

$M_n(R)$的子环，$S\cong R$，$M_n(R)-S$ 与 R 无公共元. 利用挖补定理可知，∃环$\overline{M_n(R)}=\{a\in R;A\in M_n(R)-S\}$，使得 $M_n(R)\cong\overline{M_n(R)}$且 R 是$\overline{M_n(R)}$的子环.

(ii)　$S=\left\{f\in R\{x\}\,\middle|\,\forall x\in M, f(x)\text{取 } R \text{ 中的同一值，即 } f \text{ 是常值函数}\right\}$是 $R\{x\}$的子环，$S\cong R$，$R\{x\}-S$ 与 R 无公共元. 由挖补定理，∃环$\overline{R\{x\}}=\{a\in R;f\in R\{x\}-S\}$，使得 $R\{x\}\cong\overline{R\{x\}}$且 R 是$\overline{R\{x\}}$的子环.

8. 证明：

1)　任一有单位元 1 的环 R 都同构于一自同态环.

2)　任意环 R 与一自同态环的子环同构.

证　1)　设 E 是加群 R 的所有自同态作成的环，即 E 是加群 R 的自同态环（见第九章，三，10）. 其代数运算为：$\forall f,g\in E$，$\forall x\in R$，

$$(f+g)(x)=f(x)+g(x),\ (fg)(x)=f(g(x)).$$

取定 $a\in R$，$f_a:x\to ax$ 是加群 R 的一个自同态. 事实上，f_a 显然是 R 到 R 的一个映射. 又 $\forall x,y\in R$，

$$f_a(x+y)=a(x+y)=ax+ay=f_a(x)+f_a(y),$$

从而 f_a 是加群 R 的一个自同态，即 $f_a\in E$. 作集 $\bar{E}=\left\{f_a\,\middle|\,a\in R\right\}$，则 $\bar{E}\subset E$ 且 $f_0\in\bar{E}$，从而 $\bar{E}\neq\varnothing$. $\forall f_a,f_b\in\bar{E}$，$\forall x\in R$，

$$(f_a-f_b)(x)=f_a(x)-f_b(x)=ax-bx=(a-b)x=f_{a-b}(x),$$

即 $f_a-f_b=f_{a-b}\in\bar{E}$.

$$(f_af_b)(x)=f_a(f_b(x))=f_a(bx)=a(bx)=(ab)(x)=f_{ab}(x),$$

即 $f_af_b=f_{ab}\in\bar{E}$. 所以 $\bar{E}$ 是 E 的子环. 称 $\bar{E}$ 为自同态环. 显然$\phi:a\to f_a$ 是环 R 到环 $\bar{E}$ 的满射. 又 $\forall\ a,b\in R$，$\phi:a\to f_a,b\to f_b$，有

$$\phi:a+b\to f_{a+b}=f_a+f_b,\ ab\to f_{ab}=f_af_b,$$

从而ϕ是同态满射且ϕ是单射，因为，$\forall a,b\in R$，若 $f_a=f_b$，即 $\forall x\in R$，有 $ax=bx$. 因 R 有单位元 1，当然有 $a1=b1$，即 $a=b$，从而ϕ是单射. 于是ϕ是环 R 与自同态环 $\bar{E}$ 间的一个同构映射. 所以 $R\overset{\phi}{\cong}\bar{E}$.

2)　若 R 有单位元，则由 1)知命题成立.

若 R 无单位元，则由第十一章，三，7，③知，R 可以嵌入一个有单位元的环$\bar{R}$. 由 1)知 $\bar{R}$ 与一自同态环 $\bar{E}$ 同构. 设ϕ是 $\bar{R}$ 与 $\bar{E}$ 间的同构映射，作集 $\bar{S}=\left\{\phi(x)\,\middle|\,x\in R\right\}\subset\bar{E}$，则环 $R\cong\bar{S}$. 因 R 是$\bar{R}$ 的子环，故 $\bar{S}$ 也是环且是 $\bar{E}$ 的子环. 所以 R 与自同态环 $\bar{E}$ 的子环 $\bar{S}$ 同构.

注　该命题与群论中 Cayley 定理相类似. 即自同态环在环论中的地位与变换群在群论中的地位相当.

9. 求证：

1） 域 F 与其子域 F' 的特征相等.

2） 设域 $F\cong$域 $\bar{F}$，ch $F=$素数 p，则 ch $\bar{F}=p$.

3） 设 F 是域，ch $F=$素数 p，x 是 F 上未定元，则 ch $F[x]=p$.

证 1） 由第十一章，一，4，1）及第十一章，一，5，2）知，域 F 与其子域 F' 有相同的零元 0 和单位元 1，又 F 与 F' 的特征分别是 F 与 F' 的单位元对于加法来说的阶，所以 ch $F=$ ch F'.

2） 因 ch $F=$素数 p，故域 F 中的单位元 1 对于加法来说的阶为 p. 由第五章，二，1，注 2）知，域 $\bar{F}$ 中的单位元 $\bar{1}$ 对于加法来说的阶也是 p，所以 ch $\bar{F}=p$.

3） 由第十一章，二，7，$F[x]$ 是整环. 域 F 是 $F[x]$ 的非零子整环，从而由第十一章，一，4，1）及第十一章，一，5，1）知，$F[x]$ 与 F 有相同的零元和单位元，所以 ch $F[x]=$chF$=p$.

注 1） 除环与其子除环的特征相等. 整环 R 与其子整环 $S(\neq\{0\})$ 的特征相等.

2） 因域 $\mathbb{Z}_p$（p 是素数）的特征为 p（见第十章，一，5，6）），由本题 3）知 ch $\mathbb{Z}_p[x]=p$. 此例说明，存在无限的环 $\mathbb{Z}_p[x]$，而其特征不是无限大. 因而此例也说明了第四章，二，6 的逆命题不成立.

10. 设域 F 的特征是素数 p，证明

$$R=\left\{n1\,\middle|\,n\text{ 是整数},1\text{ 是 }F\text{ 的单位元}\right\}$$

是 F 的子域.

证一 显然 $R\subset F$ 且 R 有非零元 $1\cdot 1=1$.

1） $\forall\, n1,m1\in R,\ n1-m1=(n-m)1\in R$.

2） $\forall\, n1\in R,\ n1\neq 0$. 因 ch $F=p$，故 $p\nmid n$（不然，若 $p\,|\,n$，则 $\exists\, q\in\mathbb{Z}$，使得 $n=qp$，从而 $n1=qp1=q0=0$，矛盾）. 又 p 是素数，于是 $(n,p)=1$，因此 $\exists\, h,k\in\mathbb{Z}$，使得 $hn+kp=1$，即 $hn1+kp1=1\cdot 1$. 因 $p1=0$，故 $(h1)(n1)=1$ 且 $(n1)(h1)=1$，其中 1 是 R 的单位元. 从而 $n1$ 有逆元 $(n1)^{-1}=h1\in R$. $\forall\, m1,n1\in R,\ n1\neq 0$，

$$(m1)(n1)^{-1}=(m1)(h1)=(mh)1\in R.$$

所以 R 是 F 的子域.

证二 $\forall\, n1\in R$，有 $n=qp+r,\ 0\leqslant r<p$. 从而

$$n1=(qp+r)1=qp1+r1=q0+r1=r1.$$

于是 R 里最多有 p 个元：$01=0,1\cdot 1=1,2\cdot 1,\cdots,(p-1)1$.

另一方面，若 $n_1\neq n_2,\ 0\leqslant n_i\leqslant p-1,\ i=1,2$，则 $n_11\neq n_21$. 不然，假如 $n_11=n_21$，则 $(n_1-n_2)1=0$. 因 ch $F=p$，故 $p\,|\,n_1-n_2$，但 $0\leqslant n_i\leqslant p-1,\ i=1,2$，从而 $|n_1-n_2|<p$. 因此 $n_1-n_2=0$，即 $n_1=n_2$. 矛盾. 于是 R 里恰有 p 个元.

因 $p\geqslant 2$，故 R 至少有两个元. 易证 R 是 F 的子环.

$\forall\, n1,m1\in R,\ n1\neq 0$，若 $(n1)(m1)=0$，即 $nm1=0$，从而 $p\,|\,nm$. 因 $n1\neq 0$，故 $p\nmid n$. 又 p 是素数，因此 $p\,|\,m$，即 $m1=0$. 于是 R 无零因子.

综上，R 是一个至少有两个元而且没有零因子的有限环. 因 $R\subset$域 F，故 R 是交换环. 所以，由第十章，二，3，R 是 F 的子域.

注 设 F 是整环，则

$$R=\left\{n1 \middle| n\in\mathbb{Z},1\text{ 是 }F\text{ 的单位元}\right\}$$

是 F 的子整环.

四、思考问题

1. 试判断下面各命题是否正确.

1)　设 A 是环 R 的一个子集,

$$N=\left\{S \middle| S\text{ 是 }R\text{ 的子环且 }S\supset A\right\},$$

则 $\{0\}\in N$ 或 $A\in N$.

2)　设 F 是一个域,可把 F 看成环.若 R 是 F 的子环,则 R 是一个域.

3)　设 n 是整数,则 $n\mathbb{Z}=\left\{nq \middle| q\in\mathbb{Z}\right\}$ 是整数环 $\mathbb{Z}$ 的子整环.

4)　$\mathbb{Z}_8$ 与 $\mathbb{Z}_4$ 同态.

5)　ϕ: $n\to(n,0)$ 是整数环 $\mathbb{Z}$ 到 $\mathbb{Z}\times\mathbb{Z}=\left\{(n,m) \middle| n,m\in\mathbb{Z}\right\}$ 的一个同态满射.

6)　恰含两个元的域 F 必与 $\mathbb{Z}_2$ 同构.

7)　恰含三个元的整环必与 $\mathbb{Z}_3$ 同构.

8)　设 P 是域 F 上 n 阶可逆矩阵,则 ϕ: $X\to P^{-1}XP$ 是环 $M_n(F)$ 的一个自同构.

9)　设 R 是一个有单位元的交换环,则 R 中没有 R 上的未定元.

10)　设 R 是一个有单位元的交换环,x 是 R 上未定元,$f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$,$a_n\neq0$.称 a_n 为 $f(x)$ 的最高系数.将 $f(x)$ 的次数 n 记为 $\deg f(x)$.若 $f(x),g(x)\in R[x]$.当 $f(x)\neq0,g(x)\neq0,f(x)+g(x)\neq0,f(x)g(x)\neq0$ 时,

$$\deg\,(f(x)+g(x))\leqslant\max(\deg f(x),\deg g(x)),$$

$$\deg\,(f(x)g(x))\leqslant\deg f(x)+\deg g(x).$$

当 R 是整环,$f(x)\neq0,g(x)\neq0$ 时,

$$\deg\,(f(x)g(x))=\deg f(x)+\deg g(x).$$

11)　设 R 是一个整环,x 是 R 上未定元,则

$$f(x)\text{是 }R[x]\text{的可逆元}\Leftrightarrow f(x)\in R\text{ 且 }f(x)\text{是 }R\text{ 的可逆元}.$$

2. 试证明下面各题中的 S 是环 R 的子环.

1)　R 是有理数环,$S=\left\{\frac{a}{b}\in R \middle| a,b\in\mathbb{Z},p\nmid b\right\}$,其中 p 是素数.

2)　$R=2\mathbb{Z}$,$S=6\mathbb{Z}$.

3)　R 是有理数环,$S=\left\{xm \middle| x\in R\right\}$,其中 m 是一个非零整数.

4)　$R=\left\{\begin{pmatrix}a&0\\0&a\end{pmatrix} \middle| a\in\mathbb{C}\right\}$,　$S=\left\{\begin{pmatrix}n&0\\0&n\end{pmatrix} \middle| n\in\mathbb{Z}\right\}$.

5)　$R=\left\{\begin{pmatrix}a&0\\0&b\end{pmatrix} \middle| a,b\in\mathbb{C}\right\}$,　$S=\left\{\begin{pmatrix}a&0\\0&a\end{pmatrix} \middle| a\in\mathbb{C}\right\}$.

6)　$R=\left\{\begin{pmatrix}a&b\\0&c\end{pmatrix} \middle| a,b,c\in\mathbb{C}\right\}$,　$S=\left\{\begin{pmatrix}a&0\\0&b\end{pmatrix} \middle| a,b\in\mathbb{C}\right\}$.

7） $R=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a,b\in \mathbb{C}\right\}$， $S=\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| a\in \mathbb{C}\right\}$.

8） $R=M_2(\mathbb{C})$， $S=\left\{\begin{pmatrix} a & a \\ 0 & 0 \end{pmatrix} \middle| a\in \mathbb{Q}\right\}$.

9） $R=M_n(F)$，其中 F 是一个域. S 是 $M_n(F)$ 中所有最后 $k(k\leqslant n)$ 行的元全为零的 n 阶矩阵作成的集.

10） $R=\mathbb{Z}[x]$， $S=2\mathbb{Z}[x]$.

11） $R=\mathbb{R}[x]$， $S=\mathbb{Z}[x]$.

12） $R=F[x_1,x_2,\cdots,x_n]$，其中 F 是域，$S=F[x_1]$.

3. 证明：

1） 已知 $\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}$ 是二次方程 $x^2+x+1=0$ 在复数域 $\mathbb{C}$ 中的一个根，则 $\mathbb{Q}(\omega)=\{a+b\omega \mid a,b\in \mathbb{Q}\}$ 是 $\mathbb{C}$ 的一个子域.

2） 设 F 是域，σ 是 F 的一个自同态且 σ 不是 F 的零同态（若 $\forall a\in F,\sigma(a)=0$，则称 σ 为 F 的零同态），则 $S=\{a\in F \mid \sigma(a)=a\}$ 是 F 的子域.

4. 设 a 是环 R 的一个固定元，证明：

1） $S=\{ra \mid r\in R\}$ 是 R 的一个子环.

2） $S=\{x\in R \mid xa=x\}$ 是 R 的一个子环.

3） $S=\{x\in R \mid xa=0\}$ 是 R 的一个子环.

5. 证明：环（整环、除环、域）R 的子环（整环、除环、域）S_1 与 S_2 的交 $S_1\cap S_2$ 仍是 R 的子环（整环、除环、域）.

6. 求出模 8 的剩余类环 $\mathbb{Z}_8$ 的所有子环.

7. 设 R 是一个有单位元 $1(\neq 0)$ 的环，证明：R 上 n 阶全矩阵环 $M_n(R)$ 的中心

$$Z=\left\{\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix} \middle| a\in R,\forall x\in R,ax=xa\right\}$$

$$\left(=\left\{a\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \middle| a\in R \text{ 的中心}\right\}\right).$$（矩阵中主对角线外的元素都是 0.）

8. 证明：

1） 设 $a\in$ 环 R，则 $Z(a)=\{x\in R \mid xa=ax\}$ 是 R 的子环. 称 $Z(a)$ 是元 a 在 R 内的中心化子（见第八章，三，15，1））.

2） 设 $S\subset$ 环 R，$S\neq\varnothing$，则 $Z(S)=\{x\in R \mid \forall s\in S,xs=sx\}$ 是 R 的子环. 称 $Z(S)$ 是集 S 在 R 内的中心化子（见第八章，三，15，2））.

3） 设 $S_i\subset$ 环 R，$S_i\neq\varnothing$，$i=1,2$. 当 $S_1\subset S_2$ 时，$Z(S_2)\subset Z(S_1)$.

4)　设环 R 没有非零幂零元，则 R 的幂等元都在 R 的中心里.

9. 设集 $A=\{x,y,z,u,v\}$. 规定：

+	x	y	z	u	v
x	x	y	z	u	v
y	y	z	u	v	x
z	z	u	v	x	y
u	u	v	x	y	z
v	v	x	y	z	u

•	x	y	z	u	v
x	x	x	x	x	x
y	x	y	z	u	v
z	x	z	v	y	u
u	x	u	y	v	z
v	x	v	u	z	y

证明：A 作成一个环.

10. 设 R 对于+、• 来说作成一个有单位元 1 的环，记为$(R,+,\cdot)$. 由第九章，四，2，4) 知 R 对于

$$a\oplus b=a+b-1\quad,\quad a\odot b=a+b-ab$$

来说作成一个有单位元 0 的环，记为$(R,\oplus,\odot)$. 证明：$(R,+,\cdot)\cong(R,\oplus,\odot)$.

11. 证明：环 $R_1=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$ 与环 $R_2=\{a+b\sqrt{3}\mid a,b\in\mathbb{Z}\}$ 间不可能有同构映射.

12. 设无零因子的交换环 R 的特征是素数 p，证明：$\phi: a\to a^p$ 是 R 的单射的自同态.

13. 设 F 是特征为素数 p 的域. 证明：集合 $F^p=\{a^p\mid a\in F\}$ 是 F 的子域.

14. 集 $G=\{(s_1,s_2\cdots,s_n)\mid s_i\in\mathbb{Z}\}$ 对于

$$(s_1,s_2,\cdots,s_n)=(t_1,t_2,\cdots,t_n)\Leftrightarrow s_i=t_i,i=1,2,\cdots,n,$$

$$(s_1,s_2,\cdots,s_n)+(t_1,t_2,\cdots,t_n)=(s_1+t_1,s_2+t_2,\cdots,s_n+t_n)$$

来说作成一个加群. 设

$$e_i=(0,\cdots,0,1,0,\cdots,0)\in G,$$

$i=1,2,\cdots,n$. 又设 E 是加群 G 的自同态环(见第九章，三，10). $\forall f\in E$，$f(e_i)\in G$. 若

$$f(e_i)=a_{1i}e_1+a_{2i}e_2+\cdots+a_{ni}e_n=\sum_{j=1}^{n}a_{ji}e_j,$$

$a_{ji}\in\mathbb{Z}$，$i=1,2,\cdots,n$. 显然 $f(e_i)$的表达式唯一，即 a_{ji} 由 $f(e_i)$唯一确定. 证明：

$$\phi: f\to\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\a_{21}&a_{22}&\cdots&a_{2n}\\\vdots&\vdots&&\vdots\\a_{n1}&a_{n2}&\cdots&a_{nn}\end{pmatrix}=(a_{ij})_n$$

是环 E 与 $\mathbb{Z}$ 上 n 阶全矩阵环 $M_n(\mathbb{Z})$间的一个同构映射.

15. 求出 $\mathbb{Z}_2$ 到 $\mathbb{Z}$ 的所有的同态映射.

16. 设 $\mathbb{C}$ 是复数域，$M=\left\{\begin{pmatrix}a&b\\-b&a\end{pmatrix}\middle| a,b\in\mathbb{R}\right\}$是一个域. 证明：使 $\forall\ a\in\mathbb{R}$，$a\to\begin{pmatrix}a&0\\0&a\end{pmatrix}$的 $\mathbb{C}$ 与 M 间的同构映射有且只有两个：ϕ_1 与ϕ_2，使

$$\phi_1(a+bi)=\begin{pmatrix}a & b\\ -b & a\end{pmatrix},\quad \phi_2(a+bi)=\begin{pmatrix}a & -b\\ b & a\end{pmatrix}.$$

17. 在$\mathbb{Z}_3$上，求出：

1） $([2]x^2+[1]x-[2])^2$.

2） 线性方程组

$$\begin{cases}x_1+x_2 \qquad +x_4=1\\ \qquad x_2+x_3+x_4=0\\ x_1 \qquad +x_3 \qquad =1\end{cases}$$

的所有解.

18. 设$\phi: a\to\bar{a}$ 是环 R 到环 $\bar{R}$ 的一个同态映射. 证明：$\psi: (a_{ij})\to(\bar{a}_{ij})$是环 $M_n(R)$到$M_n(\bar{R})$的一个同态映射.

19. 设域 F 中任一非零元 x 有 $x+x\neq0$. 又设ϕ是 F 到自身的一个满射，使$\phi(1)=1$. 且$\forall x,y\in F$，有$\phi(x+y)=\phi(x)+\phi(y)$，$\forall x\in F, x\neq0$，有$\phi(x)\phi(x^{-1})=1$. 证明：$\phi$是域 F 的一个自同构.

第十二章　理想、剩余类环、同态与理想

一、基本问题问答

1. 回答下列问题.

1)　理想的定义是什么？

2)　环 R 的理想$\mathfrak{A}$是加群 R 的子加群吗？反之，对吗？

3)　环 R 的理想$\mathfrak{A}$是环 R 的子环吗？反之，对吗？

答　1)　设$\mathfrak{A}$是环 R 的非空子集，则

$\mathfrak{A}$是 R 的理想 $\Leftrightarrow$ (i)　$a,b\in\mathfrak{A}\Rightarrow a-b\in\mathfrak{A}$,

(ii)　$a\in\mathfrak{A}, r\in R\Rightarrow ra, ar\in\mathfrak{A}$

$\Leftrightarrow$ (i)　$a,b\in\mathfrak{A}\Rightarrow a-b\in\mathfrak{A}$,

(ii)　$R\mathfrak{A}\subset\mathfrak{A}, \mathfrak{A}R\subset\mathfrak{A}$.

2)　环 R 的理想$\mathfrak{A}$是加群 R 的子加群. 反之，不对. 例，整数加群 $\mathbb{Z}$ 是有理数加群 $\mathbb{Q}$ 的子加群，但整数环 $\mathbb{Z}$ 不是有理数环 $\mathbb{Q}$ 的理想，因取 $\frac{1}{2}\in\mathbb{Q}$，$3\in\mathbb{Z}$，而 $\frac{1}{2}\cdot 3\,\overline{\in}\,\mathbb{Z}$.

3)　环 R 的理想$\mathfrak{A}$是环 R 的子环. 反之，不对. 见本题2)中的例. 又例，$\left\{\begin{pmatrix} a & b \\ 0 & c\end{pmatrix}\middle| a,b,c\in\mathbb{Z}\right\}$ 是 $M_2(\mathbb{Z})$ 的子环，但不是理想. 理想比子环对于乘法要求有更强的封闭性.

2. 环 R 一定有理想吗？

答　环 R 一定有理想 $\{0\}$ 与 R. 称 $\{0\}$ 与 R 为 R 的当然理想. 称 $\{0\}$ 为 R 的零理想，称 R 为 R 的单位理想. 不是 R 的当然理想的理想称为 R 的真理想.

设$\mathfrak{A}$是环 R 的理想，有 $R\mathfrak{A}\subset\mathfrak{A}$，$\mathfrak{A}R\subset\mathfrak{A}$. 若 R 有单位元，则$\mathfrak{A}\subset R\mathfrak{A}$，$\mathfrak{A}\subset\mathfrak{A}R$. 于是 $R\mathfrak{A}=\mathfrak{A}R=\mathfrak{A}$，因此 R 是理想的乘法单位元，这是称 R 为单位理想的一个原因.

3. 证明：

1)　设 R 是环，$a\in R$，由 a 生成的主理想

$(a)=\left\{x_1ay_1+\cdots+x_may_m+sa+at+na \,\middle|\, m\text{ 是正整数}, x_i, y_i, s, t\in R, n\text{ 是整数}\right\}$

是包含 a 的最小的理想.

2)　设 R 是环，若 $a\in R$ 的中心 Z，则 a 生成的主理想

$$(a)=\left\{ra+na \,\middle|\, r\in R, n\in\mathbb{Z}\right\}.$$

3)　设 R 是有单位元的环，且 $a\in R$ 的中心 Z，则

$$(a)=\left\{ra \,\middle|\, r\in R\right\}=Ra=aR.$$

证　1)　设$\mathfrak{A}$是 R 的一个理想，$a\in\mathfrak{A}$，则

$(a)\subset\mathfrak{A}$．事实上，$\forall\, x_1ay_1+\cdots+x_may_m+sa+at+na\in(a)$，因 $a\in\mathfrak{A}$，$\mathfrak{A}$是理想，故 $x_1ay_1,\cdots,x_may_m,sa,at\in\mathfrak{A}$. 又$\mathfrak{A}$是加群，从而 $na\in\mathfrak{A}$，且 $x_1ay_1+\cdots+x_may_m+sa+at+na\in\mathfrak{A}$. 所以$(a)\subset\mathfrak{A}$.

2） 由 a 与 R 中每个元都可换，即得结论.

3） 由 $na=n(1a)=(n1)a$，其中 $n1\in R$，可得结论.

注 1） 主理想是环 R 的一类构造简单，容易掌握的理想．特别是，当 R 是有单位元 1 的交换环时，主理想的构造更为简单.

2） 若$\mathfrak{A}$是环 R 的理想，$a\in\mathfrak{A}$，则由本题 1)知$(a)\subset\mathfrak{A}$.

3） 当 R 是有单位元的交换环时，由 $a_1,a_2,\cdots,a_m$ 生成的理想

$$(a_1,a_2,\cdots,a_m)=\left\{\sum_{i=1}^{m} r_i a_i \,\middle|\, r_i\in R\right\}.$$

4. 试判断以下各命题是否正确.

1） 环 R 的中心 Z 是 R 的理想.

2） 设$\mathfrak{A}$是环 R 上一元多项式环 $R[x]$的一个理想，则 $R\subset\mathfrak{A}$.

3） 除环 R 除了$\{0\}$与 R 以外，没有其他的左（右）理想（见第十二章，二，6）.

4） 设$\mathfrak{A}$，$\mathfrak{B}$是环 R 的两个理想，则$\mathfrak{A}\mathfrak{B}\subset\mathfrak{A}\cap\mathfrak{B}$，其中$\mathfrak{A}\mathfrak{B}=\left\{ab\,\middle|\,a\in\mathfrak{A},b\in\mathfrak{B}\right\}$.

5） 设$\mathfrak{A}$是环 R 的理想，则 $M_n(\mathfrak{A})$是 $M_n(R)$的理想.

6） 每一个环都至少有一个主理想.

7） 设 R 是有单位元 1 的环，则 R 是由单位元 1 生成的主理想(1).

8） 设$\mathfrak{A}$是环 R 的理想，$\mathfrak{A}$没有单位元，则$\mathfrak{A}$不是主理想.

9） 设 R 是有单位元 1 的交换环，则

$$a\text{ 是环 }R\text{ 的可逆元}\Leftrightarrow(a)=R=(1).$$

10） 设 R 是有单位元 1 的环，$\mathfrak{A}$是 R 的理想，则

$$\mathfrak{A}=R\Leftrightarrow 1\in\mathfrak{A}.$$

11） 设 R 是有单位元 1 的环，$\mathfrak{A}$是 R 的理想，$\mathfrak{A}\neq\{0\}$，R 中有可逆元，则

$$\mathfrak{A}\neq R\Leftrightarrow\mathfrak{A}\text{不含 }R\text{ 的可逆元}.$$

12） 设 $R[x]$是环 R 上的一元多项式环，则 $R[x]$的主理想$(x)=\left\{rx\,\middle|\,r\in R\right\}$.

13） 设 R 是有单位元的交换环，S 是加群 R 的子加群，且 S 是由 a 生成的循环群. 则 S 是 R 的由 a 生成的主理想.

14） 环 R 的任一理想都是 R 的主理想.

15） 环 R 的模理想$\mathfrak{A}$的剩余类环 $R/\mathfrak{A}$是加群 R 的对于不变子群$\mathfrak{A}$的商群.

16） 设ϕ是环 R 到环 $\overline{R}$ 的同态满射，A，B 是 R 的子环，$\overline{A}$，$\overline{B}$ 分别是 A，B 在ϕ下的象. 若 $\overline{A}=\overline{B}$，则 $A=B$.

17） 设ϕ是环 R 到环 $\overline{R}\neq\{\overline{0}\}$的同态映射，$R$ 有单位元 1，且$\phi(1)$是 $\overline{R}$ 的单位元$\overline{1}$. a 是 R 的可逆元，则

$$\phi(a)\text{是 }\overline{R}\text{ 的可逆元}\Leftrightarrow a\,\overline{\in}\,\ker\phi.$$

18） 设$\mathfrak{A}$是环 R 的子环，则

$$\mathfrak{A}\text{是 }R\text{ 的理想}\Leftrightarrow\exists R\text{ 到某个环 }\overline{R}\text{ 的同态满射}\phi\text{，使得}\mathfrak{A}=\ker\phi.$$

19）若ϕ是环R到环$\overline{R}$的同态映射，则$\ker\phi=\left\{a\in R \,\middle|\, \phi(a)=\overline{0}\text{，这里}\overline{0}\text{是}\overline{R}\text{的零元}\right\}$是$R$的理想.

20）若ϕ是域F到域$\overline{F}$的同态映射，且$\phi(F)\neq\{\overline{0}\}$，则$\phi$是单射.

答 1）不正确.例，由第十一章，四，7知环$M_2(\mathbb{Z})$的中心是$Z=\left\{\begin{pmatrix}a & \\ & a\end{pmatrix}\,\middle|\, a\in\mathbb{Z}\right\}$.取$\begin{pmatrix}1&2\\3&4\end{pmatrix}\in M_2(\mathbb{Z})$，$\begin{pmatrix}1&0\\0&1\end{pmatrix}\in Z$，但$\begin{pmatrix}1&2\\3&4\end{pmatrix}\begin{pmatrix}1&0\\0&1\end{pmatrix}=\begin{pmatrix}1&2\\3&4\end{pmatrix}\overline{\in} Z$.所以$Z$不是$M_2(\mathbb{Z})$的理想.

2）不正确.例，

$$\mathfrak{A}=(x)=\left\{a_1x+a_2x^2+\cdots+a_nx^n \,\middle|\, a_i\in R, n\text{是正整数}\right\}$$

是环R上的一元多项式环$R[x]$的一个理想[①].$1\in R$.但$1\overline{\in}\mathfrak{A}$.不然，若$1\in\mathfrak{A}$，则

$$1=a_1x+a_2x^2+\cdots+a_nx^n,$$

即

$$-1+a_1x+a_2x^2+\cdots+a_nx^n=0.$$

其中$-1\neq0$，从而x不是R上未定元，此为矛盾.所以$1\overline{\in}\mathfrak{A}$.即$R\not\subset\mathfrak{A}$.

3）正确.事实上，设$\mathfrak{A}$是R的一个左理想且$\mathfrak{A}\neq\{0\}$，则$\exists a\in\mathfrak{A}, a\neq0$，$\exists a^{-1}\in R$，使得$a^{-1}a=1\in\mathfrak{A}$，从而$\forall r\in R, r=r1\in\mathfrak{A}$，即$R=\mathfrak{A}$.同理可证另一情况.

4）正确.事实上，$\forall ab\in\mathfrak{A}\mathfrak{B}$，其中$a\in\mathfrak{A}, b\in\mathfrak{B}$.因$\mathfrak{A}$是理想，故$ab\in\mathfrak{A}$.因$\mathfrak{B}$是理想，故$ab\in\mathfrak{B}$，从而$ab\in\mathfrak{A}\mathfrak{B}$.所以$\mathfrak{A}\mathfrak{B}\subset\mathfrak{A}\cap\mathfrak{B}$.

5）正确.直接利用定义可证.

6）正确.因为每一个环都有主理想(0).

7）正确.事实上，显然$(1)\subset R$；反之，$\forall r\in R, r=r1\in(1)$，从而$R\subset(1)$.所以$R=(1)$.

8）不正确.例，偶数环$2\mathbb{Z}$是整数环$\mathbb{Z}$的理想，$2\mathbb{Z}$无单位元，但$2\mathbb{Z}$是$\mathbb{Z}$的主理想(2).

9）正确.事实上，$(\Rightarrow)$　显然$(a)\subset R$；反之，$\forall r\in R$，有$r=r1=r(a^{-1}a)=(ra^{-1})a\in(a)$，从而$R\subset(a)$.所以$(a)=R$.$(\Leftarrow)$　因$1\in R=(a)$，又R是交换环，故$\exists b\in R$，使得$1=ba$，从而a是R的可逆元.

该命题的逆否命题为：设R是有单位元1的交换环，则

$$a\text{不是环}R\text{的可逆元}\Leftrightarrow(a)\neq R.$$

但当R不是交换环时，a虽不是R的可逆元，却可能$(a)=R$.例，$\begin{pmatrix}1&0\\0&0\end{pmatrix}$不是环$M_2(\mathbb{Z})$的可逆元，但$\left(\begin{pmatrix}1&0\\0&0\end{pmatrix}\right)=M_2(\mathbb{Z})$.

10）正确.事实上，$(\Rightarrow)$　显然.$(\Leftarrow)$　显然$\mathfrak{A}\subset R$；反之，$\forall r\in R$，因$1\in\mathfrak{A}$，$\mathfrak{A}$是理想，故$r=r1\in\mathfrak{A}$，从而$R\subset\mathfrak{A}$.所以$\mathfrak{A}=R$.

11）正确.事实上，$(\Leftarrow)$　显然.$(\Rightarrow)$　若理想$\mathfrak{A}$含R的可逆元a，则$\exists a^{-1}\in R$，使得$1=a^{-1}a\in\mathfrak{A}$.由本题10），$\mathfrak{A}=R$.

12）不正确.因为

① 张禾瑞．近世代数基础．北京：高等教育出版社，1978.111.例2.

$$(x)=\left\{f(x)x \,\middle|\, f(x)\in R[x]\right\}=\left\{(a_0+a_1x+\cdots+a_nx^n)x \,\middle|\, a_i\in R, n \text{ 是非负整数}\right\}$$
$$=\left\{a_0x+a_1x^2+\cdots+a_nx^{n+1} \,\middle|\, a_i\in R, n \text{ 是非负整数}\right\}$$
$$=\left\{a_1x+a_2x^2+\cdots+a_mx^m \,\middle|\, a_i\in R, m \text{ 是正整数}\right\}.$$

所以$(x+1)x\in(x)$，但$(x+1)x\overline{\in}\{rx \mid r\in R\}$.

13) 不正确. 例，取 R=有理数环. 由 1 生成的 R 的循环子加群是$\{n1 \mid n\in\mathbb{Z}\}=\mathbb{Z}$. 而由 1 生成的 R 的主理想是$\{r1 \mid r\in R\}=R\neq\mathbb{Z}$.

14) 不正确. 例，环 $\mathbb{Z}[x]$的理想$(2,x)$不是主理想①.

15) 正确. 由定义可知.

16) 不正确. 例，设 $R=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix} \,\middle|\, a,b,c,d\in\mathbb{R}\right\}$，$\overline{\mathbb{R}}=\left\{\begin{pmatrix}a&b\\0&0\end{pmatrix} \,\middle|\, a,b\in\mathbb{R}\right\}$. $\phi:\begin{pmatrix}a&b\\c&d\end{pmatrix}\to\begin{pmatrix}a&b\\0&0\end{pmatrix}$是环 R 到环$\overline{R}$ 的同态满射. $A=\left\{\begin{pmatrix}a&0\\c&0\end{pmatrix} \,\middle|\, a,c\in\mathbb{R}\right\}$，$B=\left\{\begin{pmatrix}a&0\\0&d\end{pmatrix} \,\middle|\, a,d\in\mathbb{R}\right\}$是 R 的子环. A,B 在ϕ下的象都是$\left\{\begin{pmatrix}a&0\\0&0\end{pmatrix} \,\middle|\, a\in\mathbb{R}\right\}$，而 $A\neq B$. 又例，设 R 是至少含两个元的环，环 $\overline{R}=\{\bar{0}\}$. $\phi:x\to\bar{0}$ 是 R 到 $\overline{R}$ 的同态满射. R 与$\{0\}$是 R 的两个子环，它们在ϕ下的象都是$\{\bar{0}\}$，但 $R\neq\{0\}$. 又例，$\phi:a\to[a]$是整数环 $\mathbb{Z}$ 到模 n 的剩余类环 $\mathbb{Z}_n$ 的同态满射. $A=\{2kn \mid k\in Z\}$，$B=\{4hn \mid h\in\mathbb{Z}\}$都是 $\mathbb{Z}$ 的子环. A,B 在ϕ下的象都是$\{[0]\}$，但 $A\neq B$. 因 $2n\in A$，而 $2n\overline{\in}B$. 又例，$\phi:[0]\to[0],[1]\to[1],[2]\to[0],[3]\to[1]$是环 $\mathbb{Z}_4$ 到环 $\mathbb{Z}_2$ 的同态满射. $\mathbb{Z}_4$ 的两个子环：$A=\{[0]\}$，$B=\{[0],[2]\}$在ϕ下的象都是$\{[0]\}$，而 $A\neq B$.

又例，$R=\{(a,b) \mid a,b\in\mathbb{Q}\}$对于

$$(a_1,b_1)=(a_2,b_2)\Leftrightarrow a_1=a_2, b_1=b_1,$$
$$(a_1,b_1)+(a_2,b_2)=(a_1+a_2, b_1+b_2),$$
$$(a_1,b_1)(a_2,b_2)=(a_1a_2, b_1b_2)$$

作成一个环. $\phi:(a,b)\to b$ 是环 R 到有理数环 $\mathbb{Q}$ 的同态满射. $A=\{(a,b) \mid a,b\in\mathbb{Z}\}$与 $B=\{(0,b) \mid b\in\mathbb{Z}\}$是 R 的子环，它们在ϕ下的象都是整数环 $\mathbb{Z}$，但 $A\neq B$.

对于该命题适当增加条件，可使结论成立. 即：设ϕ是环 R 到环$\overline{R}$ 的同态满射，A,B 是 R 的含 $\ker\phi$的两个子环. 若$\phi(A)=\phi(B)$(见第八章，三，8)，则 $A=B$. 事实上，$\forall a\in A$，$\phi(a)\in\phi(A)=\phi(B)$，从而$\exists b\in B$，使得$\phi(a)=\phi(b)$，即$\phi(a-b)=\phi(a)-\phi(b)=0$，于是 $a-b\in\ker\phi\subset B$，因此$\exists b'\in B$，使得 $a-b=b'$，即 $a=b+b'\in B$. 所以 $A\subset B$. 同理可证 $B\subset A$. 综上，$A=B$.

17) 正确. 事实上，$(\Rightarrow)$ 若$\phi(a)$可逆，则$\phi(a)\neq\bar{0}$，其中 $\bar{0}$ 是 $\overline{R}$ 的零元，从而 $a\overline{\in}\ker\phi$. $(\Leftarrow)$ 若 $a\overline{\in}\ker\phi$，则$\phi(a)\neq\bar{0}$. 因 a 是 R 的可逆元，故$\exists a^{-1}\in R$，使得$\phi(a^{-1})\phi(a)=\phi(a^{-1}a)=\phi(1)=\bar{1}$，所以$\phi(a)$是 $\overline{R}$ 的可逆元.

---

① 张禾瑞．近世代数基础．北京：高等教育出版社，1978. 112. 例 3.

18)　正确. 事实上,($\Rightarrow$)　因$\mathfrak{A}$是 R 的理想,故 $\exists R$ 的模理想$\mathfrak{A}$的剩余类环 $R/\mathfrak{A}$,而 $\phi: a \to [a]$是 R 到 $R/\mathfrak{A}$的同态满射,且$\mathfrak{A}=\ker\phi$(见第八章,一,5,2)). ($\Leftarrow$)　若ϕ是环 R 到环 $\overline{R}$ 的同态满射,则$\mathfrak{A}=\ker\phi$是 R 的理想[①].

该命题说明,环 R 有多少个理想,环 R 就有多少个到环 R 的同态满射.

19)　正确. 事实上,由第十一章,三,3,1),$\phi(0)=\overline{0}$,从而 $0\in\ker\phi$,因此 $\ker\phi$不空且 $\ker\phi\subset R$. $\forall a,b\in\ker\phi$,有$\phi(a)=\overline{0},\phi(b)=\overline{0}$,从而$\phi(a-b)=\phi(a)-\phi(b)=\overline{0}-\overline{0}=\overline{0}$. 于是 $a-b\in\ker\phi$. $\forall a\in\ker\phi, r\in R$,有$\phi(a)=\overline{0},\phi(ra)=\phi(r)\phi(a)=\phi(r)\overline{0}=\overline{0}$. 同理$\phi(ar)=\overline{0}$,于是 $ra, ar\in\ker\phi$. 所以 $\ker\phi$是 R 的理想.

20)　正确. 事实上,由本题 19),$\ker\phi$是 F 的理想,而 F 是域,因此 F 只有零理想$\{0\}$和单位理想 F. 又$\phi(F)\neq\{\overline{0}\}$,从而 $\ker\phi\neq F$,只能 $\ker\phi=\{0\}$. $\forall a,b\in F$,若$\phi(a)=\phi(b)$,则$\phi(a-b)=\overline{0}$,于是 $a-b\in\ker\phi=\{0\}$,即 $a=b$. 所以ϕ是单射(见第十一章,三,5).

5. 回答下列问题.

1)　何谓环 R 的模理想$\mathfrak{A}$的剩余类?

2)　何谓环 R 的模理想$\mathfrak{A}$的剩余类环(或称商环或差环)?

3)　设 S 是环 R 的子环,$T=\{[x]\mid x\in R\}$,其中$[x]=x+S=\{x+s\mid s\in S\}$,法则 $[a][b]=[ab]$是否为 T 的一个代数运算?

4)　类似于群中的商群,环 R 的模理想$\mathfrak{A}$的剩余类环 $R/\mathfrak{A}$与同态有何关系?

答　1)　环 R 的理想$\mathfrak{A}$是加群 R 的子加群,而加群 R 对加法可换,从而$\mathfrak{A}$是加群 R 的不变子群,从而利用不变子群$\mathfrak{A}$可规定加群 R 的元间的一个等价关系:$\forall a,b\in R$,

$$a\sim b\Leftrightarrow a-b\in\mathfrak{A}.$$

记为 $a\equiv b(\mathfrak{A})\Leftrightarrow a-b\in\mathfrak{A}$,读作 a 同余 b 模理想$\mathfrak{A}$. 利用此等价关系～可以对加群 R 进行分类,得出的类即为$\mathfrak{A}$的陪集 $x+\mathfrak{A}=\{x+u\mid u\in\mathfrak{A}\}$,叫做模理想$\mathfrak{A}$的剩余类,记为$[x]$,即

$$[x]=x+\mathfrak{A}=\{x+u\mid u\in\mathfrak{A}\}.$$

2)　设

①　$\mathfrak{A}$是环 R 的理想;

②　$\overline{R}$ 是所有模$\mathfrak{A}$的剩余类的集合:

$$\overline{R}=\{[x],[y],\cdots\};$$

③　规定

$$[a]+[b]=[a+b],\ [a][b]=[ab].$$

可以证明 $\overline{R}$ 是一个环(注意$\mathfrak{A}$是理想这一条件的作用,它保证了如此规定的乘法是 $\overline{R}$ 的一个代数运算). 称环 $\overline{R}$ 为环 R 的模理想$\mathfrak{A}$的剩余类环,记为 $R/\mathfrak{A}$. 即

$$R/\mathfrak{A}=\{[x]\mid x\in R\}=\{x+\mathfrak{A}\mid x\in R\}.$$

注　(i)　利用环 R 的理想$\mathfrak{A}$可以作出新的环 $R/\mathfrak{A}$,由此可见理想的重要性.

(ii)　环 $R/\mathfrak{A}$的零元是$[0]=0+\mathfrak{A}$.

(iii)　$[a](\in R/\mathfrak{A})$的负元$-[a]=[-a]$.

---

① 张禾瑞. 近世代数基础. 北京:高等教育出版社,1978. 114. 定理 2.

(iv) 若 R 有单位元 1，则 $R/\mathfrak{A}$ 有单位元 $[1]=1+\mathfrak{A}$.

(v) 若 R 是交换环，则 $R/\mathfrak{A}$ 也是交换环.

(vi) 当 $\mathfrak{A}=R$ 时，

$$R/\mathfrak{A}=R/R=\{x+R \mid x\in R\}=\{R\}=\{0+R\}=\{[0]\};$$

当 $\mathfrak{A}=\{0\}$ 时，

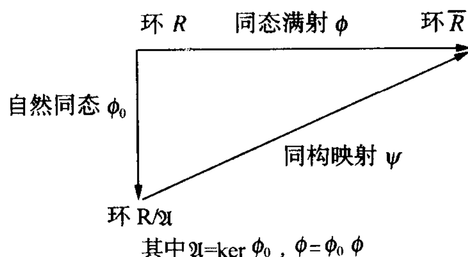
$$R/\mathfrak{A}=R/\{0\}=\{x+\{0\} \mid x\in R\}=\{\{x\} \mid x\in R\}\cong R.$$

3) 未必是. 例，$\mathbb{Z}$ 是 $\mathbb{Q}$ 的子环，但 $\mathbb{Z}$ 不是 $\mathbb{Q}$ 的理想. $T=\{[x] \mid x\in\mathbb{Q}\}$，其中 $[x]=x+\mathbb{Z}$. 取 $\frac{1}{2}+\mathbb{Z}, \frac{1}{3}+\mathbb{Z}\in T$，由规定，$\left(\frac{1}{2}+\mathbb{Z}\right)\left(\frac{1}{3}+\mathbb{Z}\right)=\frac{1}{6}+\mathbb{Z}$. 又 $\frac{1}{2}+\mathbb{Z}=\frac{3}{2}+\mathbb{Z}$，由规定，$\left(\frac{3}{2}+\mathbb{Z}\right)\left(\frac{1}{3}+\mathbb{Z}\right)=\frac{1}{2}+\mathbb{Z}$. 因 $\frac{1}{6}-\frac{1}{2}\notin\mathbb{Z}$，故 $\frac{1}{6}+\mathbb{Z}\neq\frac{1}{2}+\mathbb{Z}$. 从而在此法则：$[a][b]=[ab]$ 下，象不唯一. 所以此法则不是 T 的一个代数运算.

注 当 $\mathfrak{A}$ 是环 R 的理想时，才能保证 $R/\mathfrak{A}$ 是一个环.

4) $R\overset{\phi_0}{\sim}R/\mathfrak{A}$，$\phi_0: a\rightarrow[a]$ 是 R 到 $R/\mathfrak{A}$ 的一个同态满射，称为自然同态. ϕ_0 的核 $\ker\phi_0=\{a\in R \mid \phi_0(a)=\bar{0}$，这里 $\bar{0}$ 是 R/a 的零元$\}=\mathfrak{A}$（ϕ_0 的核即为把 ϕ_0 看成是加群 R 到加群 $R/\mathfrak{A}$ 的同态满射的核，因此由第八章，一，5，2）知 $\ker\phi_0=\mathfrak{A}$）.

另一方面，设环 $R\overset{\phi}{\sim}$环 $\bar{R}$，则 $\mathfrak{A}=\ker\phi$ 是 R 的一个理想且 $R/\mathfrak{A}\overset{\psi}{\cong}\bar{R}$（见下图）.



其中 $\mathfrak{A}=\ker\phi_0$，$\phi=\phi_0\phi$

注 ① 此命题称为环的同态基本定理. 它一方面指出环 R 的模理想的剩余类环必为 R 在同态满射下的象；另一方面指出在同构意义下，环 R 在同态满射下的象是 R 的模理想的剩余类环. 也就是说，环 R 的所有的模理想的剩余类环已经穷尽了 R 的所有的在同态满射下的象. 如果掌握了环 R 的所有的理想，也就掌握了 R 的所有的在同态满射下的象. 理想可以决定环 R 的所有的同态象. 由此可见理想与模理想的剩余类环在环的结构理论中的重要作用.

② 由上述可知，只要把群和不变子群分别改成环和理想，那么关于群的各种同构定理都可移植到环上来. 应注意的是：群的不变子群 N 的陪集一般写成乘法形式 aN，而环的理想 $\mathfrak{A}$ 的陪集（即模 $\mathfrak{A}$ 的剩余类）要写成加法形式 $x+\mathfrak{A}$.

例 1 可将第八章，二，8 移植到环上来，即：设环 $R\overset{\phi}{\sim}$环 $\bar{R}$，$\bar{\mathfrak{A}}$ 是 $\bar{R}$ 的理想，$\phi^{-1}(\bar{\mathfrak{A}})=\mathfrak{A}$（见第八章，三，8），则 $R/\mathfrak{A}\cong\bar{R}/\bar{\mathfrak{A}}$. 事实上，仿第八章，二，8 的证明可知，$\psi: a\rightarrow[\phi(a)]=\phi(a)+\bar{\mathfrak{A}}$ 是 R 到 $\bar{R}/\bar{\mathfrak{A}}$ 的一个同态满射且 $\ker\psi=\mathfrak{A}$. 由同态基本定理，$R/\mathfrak{A}\cong\bar{R}/\bar{\mathfrak{A}}$.

或直接证明：$\forall a\in R$，$\psi: a+\mathfrak{A}\rightarrow\phi(a)+\bar{\mathfrak{A}}$ 是 $R/\mathfrak{A}$ 与 $\bar{R}/\bar{\mathfrak{A}}$ 间的一个同构映射.

或如下证明：因 $R\overset{\phi}{\sim}\bar{R}$，又 $\bar{R}\overset{\phi_0}{\sim}\bar{R}/\bar{\mathfrak{A}}$，这里$\phi_0$ 是自然同态，故 $R\overset{\phi_0\phi}{\cong}\bar{R}/\bar{\mathfrak{A}}$（见第二章，二，5）且 $\ker(\phi_0\phi)=\mathfrak{A}$. 由同态基本定理，即可得结论.

例，环 $\mathbb{Z}\overset{\phi}{\sim}$环 $\mathbb{Z}_6$，其中$\phi: n\to[n]$是自然同态. $\bar{\mathfrak{A}}=\{[0],[3]\}$是 $\mathbb{Z}_6$的理想，$\phi^{-1}(\bar{\mathfrak{A}})=\{3q\,|\,q\in\mathbb{Z}\}=3\mathbb{Z}$，从而 $\mathbb{Z}_3=\mathbb{Z}/3\mathbb{Z}\cong\mathbb{Z}_6/\{[0],[3]\}$.

由此例 1 可立得下面命题：设环 $R\overset{\phi}{\sim}$环 $\bar{R}$，$\mathfrak{A}$是 R 的含 $\ker\phi$的理想，$\phi(\mathfrak{A})=\bar{\mathfrak{A}}$，则$R/\mathfrak{A}\cong\bar{R}/\bar{\mathfrak{A}}$. 事实上，因$\phi(\mathfrak{A})=\bar{\mathfrak{A}}$，又$\mathfrak{A}\supset\ker\phi$，故由第八章，二，7，注 3）知，$\phi^{-1}(\bar{\mathfrak{A}})=\mathfrak{A}$. 从而由本例 1，有 $R/\mathfrak{A}\cong\bar{R}/\bar{\mathfrak{A}}$.

例 2　可将第八章，四，46 移植到环上来，即：设$\mathfrak{A}$和$\mathfrak{B}$都是环 R 的理想且$\mathfrak{A}\subset\mathfrak{B}$，则$\mathfrak{B}/\mathfrak{A}$是 $R/\mathfrak{A}$的理想且 $R/\mathfrak{B}\cong(R/\mathfrak{A})/(\mathfrak{B}/\mathfrak{A})$. 事实上，仿第八章，四，46 的证明，可知：$\forall a\in R$，$\phi: a+\mathfrak{A}\to a+\mathfrak{B}$是 $R/\mathfrak{A}$到 $R/\mathfrak{B}$的一个同态满射且 $\ker\phi=\mathfrak{B}/\mathfrak{A}$. 由同态基本定理知结论成立.

例，设 $r\,|\,m$，则 $\mathbb{Z}/r\cong(\mathbb{Z}/(m))/((r)/(m))$. 因为主理想$(m)$，$(r)$都是整数环 $\mathbb{Z}$ 的理想且因 $r\,|\,m$，故$(m)\subset(r)$，所以由此例 2 可得结论.

例 3　可将第八章，四，47 移植到环上来，即：设$\mathfrak{A}$，$\mathfrak{B}$都是环 R 的理想，则

$$R/(\mathfrak{A}+\mathfrak{B})\cong(R/\mathfrak{A})/((\mathfrak{A}+\mathfrak{B})/\mathfrak{A}).$$

其中$\mathfrak{A}+\mathfrak{B}=\{a+b\,|\,a\in\mathfrak{A},b\in\mathfrak{B}\}$. 事实上，由$\mathfrak{A}+\mathfrak{B}$是 R 的理想，$\mathfrak{A}\subset\mathfrak{A}+\mathfrak{B}$及上面例 2 可知命题成立.

例 4　可将第八章，四，48 移植到环上来，即设$\mathfrak{A}$是环 R 的理想，S 是 R 的子环，则$\mathfrak{A}\cap S$是 S 的理想且 $S/(\mathfrak{A}\cap S)\cong(\mathfrak{A}+S)/\mathfrak{A}$. 事实上，仿第八章，四，48 的证明，可知；$\forall s\in S$，$\phi$：$s\to s+\mathfrak{A}$是 S 到$(\mathfrak{A}+S)/\mathfrak{A}$的一个同态满射且 $\ker\phi=\mathfrak{A}\cap S$，从而由同态基本定理得证.

或如下证明：$\forall s\in S, a\in\mathfrak{A}, \phi: a+s\to s+(\mathfrak{A}\cap S)$是$\mathfrak{A}+S$ 到 $S/(\mathfrak{A}\cap S)$的一个同态满射且 $\ker\phi=\mathfrak{A}$，从而由同态基本定理得证.

或直接证明：$\forall s\in S, \phi: s+(\mathfrak{A}\cap S)\to S+\mathfrak{A}$是 $S/(\mathfrak{A}\cap S)$到$(\mathfrak{A}+S)/\mathfrak{A}$的一个同构映射.

6. 设 R 是除环，$\bar{R}$ 是环且 $R\overset{\phi}{\sim}\bar{R}$，证明：$R$ 的同态象 $\bar{R}$ 或与 R 同构，或为零环$\{\bar{0}\}$.

证　因除环 R 只有零理想$\{0\}$和单位理想 R，故 $\ker\phi=\{0\}$或 R. 由同态基本定理，$R/\{0\}\cong\bar{R}$ 或$R/R\cong\bar{R}$. 而

$$R/\{0\}=\{\{x\}\,|\,x\in R\}\cong R,\ R/R=\{[0]\},$$

于是 $\bar{R}\cong R$ 或$\bar{R}\cong\{[0]\}$. 所以命题得证.

注　1）　设 R 是除环，$\bar{R}$ 是环且 $R\overset{\phi}{\sim}\bar{R}$，则由该命题知，$\phi$或是同构映射或是零同态.

2）　当 R 是域时，命题也成立.

3）　设 R 与 $\bar{R}$ 都是除环（域）且 $R\overset{\phi}{\sim}\bar{R}$. 因 $\bar{R}$ 是除环（域），故ϕ不是零同态，从而ϕ是 R 到 $\bar{R}$ 的同构映射. 这就给出了第十一章，三，5 的又一个证明.

7. 证明：整数环 $\mathbb{Z}$ 的模理想(n)的剩余类环 $R/(n)$就是整数环 $\mathbb{Z}$ 的模 n 的剩余类环 $\mathbb{Z}_n$.

证　$\forall[x]\in R/(n)$，因$[x]=x+(n)=\{x+nk/k\in\mathbb{Z}\}$，故$[x]\in\mathbb{Z}_n$；反之，$\forall[a]\in\mathbb{Z}_n$，因$[a]=\{a+nq\,|\,q\in\mathbb{Z}\}=a+(n)$，故$[a]\in R/(n)$. 所以 $R/(n)=\mathbb{Z}_n$.

注 一般的环 R 的模理想$\mathfrak{A}$的剩余类环 $R/\mathfrak{A}$是特殊的整数环 $\mathbb{Z}$ 的模 n 的剩余类环 $\mathbb{Z}_n$ 的推广. 这也是 $R/\mathfrak{A}$的名称的由来.

8. 设ϕ是环 R 到环 $\overline{R}$ 的同态映射，证明：

1） S 是 R 的子环 $\Rightarrow \phi(S)$是 $\overline{R}$ 的子环.

2） $\overline{S}$ 是 $\overline{R}$ 的子环 $\Rightarrow \phi^{-1}(\overline{S})$是 R 的子环.

3） $\overline{\mathfrak{A}}$是 $\overline{R}$ 的理想 $\Rightarrow \phi^{-1}(\overline{\mathfrak{A}})$是 R 的理想.

证 1） 因 S 是 R 的子环，故零元 $0\in S$，从而$\phi(0)=\overline{0}\in\phi(S)$，（见第十一章，三，3，1）），即$\phi(S)$不空. 显然$\phi(S)\subset\overline{R}$. $\forall \overline{a},\overline{b}\in\phi(S)$，由$\phi(S)$定义，$\exists a,b\in S$，使得$\phi(a)=\overline{a}$，$\phi(b)=\overline{b}$. 由$\phi$是同态映射及第十一章，三，3，2），有

$$\overline{a}-\overline{b}=\phi(a)-\phi(b)=\phi(a)+[-\phi(b)]=\phi(a)+\phi(-b)=\phi(a+(-b))=\phi(a-b),$$

$$\overline{a}\,\overline{b}=\phi(a)\,\phi(b)=\phi(ab).$$

因 S 是 R 的子环，故 $a-b,ab\in S$，从而 $\overline{a}-\overline{b},\overline{a}\,\overline{b}\in\phi(S)$，所以$\phi(S)$是 $\overline{R}$ 的子环.

2） 因 $\overline{S}$ 是 $\overline{R}$ 的子环，故零元 $\overline{0}\in\overline{S}$. 因$\phi$是 R 到 $\overline{R}$ 的同态映射，故 $\overline{0}$ 必有逆象零元 $0\in R$，从而 $0\in\phi^{-1}(\overline{S})$，即$\phi^{-1}(\overline{S})$不空. 显然$\phi^{-1}(S^{-1})\subset R$. $\forall a,b\in\phi^{-1}(\overline{S})$，由$\phi^{-1}(\overline{S})$的定义，$\exists\,\overline{a},\overline{b}\in\overline{S}$，使得$\phi(a)=\overline{a}$，$\phi(b)=\overline{b}$. 因$\phi$是同态映射，又 $\overline{S}$ 是 $\overline{R}$ 的子环，故

$$\phi(a-b)=\phi(a)-\phi(b)\in\overline{S},\ \phi(ab)=\phi(a)\phi(b)\in\overline{S},$$

所以 $a-b,ab\in\phi^{-1}(\overline{S})$. 因此$\phi^{-1}(\overline{S})$是 R 的子环.

3） 由 2）已知$\phi^{-1}(\overline{\mathfrak{A}})$是 R 的子环. $\forall r\in R$，$\forall a\in\phi^{-1}(\overline{\mathfrak{A}})$，$\exists\,\overline{a}\in\overline{\mathfrak{A}}$，使得$\phi(a)=\overline{a}$. 于是

$$\phi(ra)=\phi(r)\phi(a)=\phi(r)\overline{a}.$$

因$\phi(r)\in\overline{R}$，$\overline{a}\in\overline{\mathfrak{A}}$，又$\overline{\mathfrak{A}}$是 $\overline{R}$ 的理想，故$\phi(ra)\in\overline{\mathfrak{A}}$，从而 $ra\in\phi^{-1}(\overline{\mathfrak{A}})$. 同理 $ar\in\phi^{-1}(\overline{\mathfrak{A}})$. 所以 $\phi^{-1}(\overline{\mathfrak{A}})$是 R 的理想.

注 参看第八章，三，8，进行对比.

例 ϕ：$n\to[n]$是整数环 $\mathbb{Z}$ 到 $\mathbb{Z}$ 的模理想(7)的剩余类环 $\mathbb{Z}/(7)$的自然同态. 即 $\mathbb{Z}\overset{\phi}{\sim}\mathbb{Z}/(7)$. 偶数环 $2\mathbb{Z}$ 是 $\mathbb{Z}$ 的子环，于是$\phi(2\mathbb{Z})=\{[0],[2],[4],[6]\}$是 $\mathbb{Z}/(7)$的一个子环.

二、典型问题分析

1. 假定 R 是偶数环. 证明：所有整数 $4r(r\in R)$是 R 的一个理想$\mathfrak{A}$. 等式$\mathfrak{A}=(4)$对不对？

证 已知$\mathfrak{A}=\{4r\,|\,r\in R\}$. 因 $4\cdot 0=0\in\mathfrak{A}$，故$\mathfrak{A}\neq\varnothing$. 显然$\mathfrak{A}\subset R$. $\forall 4r_1,4r_2\in\mathfrak{A}$，其中 $r_1,r_2\in R$，有 $r_1-r_2\in R$，于是

$$4r_1-4r_2=4(r_1-r_2)\in\mathfrak{A}.$$

$\forall 4r_1\in\mathfrak{A}$，其中 $r_1\in R$，$\forall r\in R$，有 $r_1r\in R$，于是

$$(4r_1)r=r(4r_1)=4(r_1r)\in\mathfrak{A}.$$

所以$\mathfrak{A}$是 R 的一个理想.

$$\mathfrak{A}=\{4r\,|\,r\in R\}=\{4\cdot 2n\,|\,n\in\mathbb{Z}\}=\{8n\,|\,n\in\mathbb{Z}\}=\{r\cdot 8+n\cdot 8\,|\,r\in R,n\in\mathbb{Z}\}=(8).$$

即$\mathfrak{A}$是偶数环 R 的由 8 生成的主理想. 因偶数环 R 是交换环但无单位元，故

$$(4)=\left\{r\cdot 4+n\cdot 4\,\middle|\,r\in R,n\in\mathbb{Z}\right\}=\left\{4(r+n)\right\}=\left\{4q\,\middle|\,q\in\mathbb{Z}\right\}.$$

从而$\mathfrak{A}\subset(4)$. 但 $4(2k-1)\in(4)$,而 $4(2k-1)\overline{\in}\mathfrak{A}$,这里 k 是任意整数,所以$\mathfrak{A}\neq(4)$.

注 1) 若 R 是有单位元的交换环,则$\mathfrak{A}=\left\{4r\,\middle|\,r\in R\right\}$是主理想. 例,当 R 是整数环时,$\mathfrak{A}=(4)$.

2) 一般来说,设 R 是没有单位元的环,取定 $a\in R$,则$\mathfrak{A}=\left\{ar\,\middle|\,r\in R\right\}$是 R 的理想,但$\mathfrak{A}$未必是由 a 生成的主理想(a).

再举个例子. 在由 6 个模 12 的剩余类作成的无单位元的交换环 $R=\{[0],[2],[4],[6],[8],[10]\}$中,$\mathfrak{A}=\left\{[2][r]\,\middle|\,[r]\in R\right\}$是 R 的理想. 但$[2]\overline{\in}\mathfrak{A}$. 事实上,若$[2]\in\mathfrak{A}$,则$[2]=[2][r]=[2r]$,从而 $12\,|\,2r-2$,即 $6\,|\,r-1$,可是 r 只能取 0,2,4,6,8,10,此与 $6\,|\,r-1$ 矛盾. 所以$[2]\overline{\in}\mathfrak{A}$. 而$[2]\in([2])$,于是$\mathfrak{A}\neq([2])$. 如果取$\mathfrak{B}=\left\{[4][r]\,\middle|\,[r]\in R\right\}$则$\mathfrak{B}$是 R 的理想. 因$[4]=[16]=[4][4]\in\mathfrak{B}$,故$([4])\subset\mathfrak{B}$,显然$\mathfrak{B}\subseteq([4])$. 于是$\mathfrak{B}=([4])$.

2. 假定 R 是整数环. 证明:$(3,7)=(1)$.

证 因 3,7 互素,故∃整数 u,v,使得 $3u+7v=1$. 因 $3u+7v\in(3,7)$,故 $1\in(3,7)$,所以$(3,7)=(1)$(见第十二章,一,4,7)).

3. 假定 R 是有理数域. 证明:$(2,x)$是 $R[x]$的一个主理想.

证一 因 2 与 x 互素,又 R 是有理数域,故∃$u(x),v(x)\in R[x]$,使得 $2u(x)+xv(x)=1$. 因 $R[x]$是有单位元的交换环,故

$$2u(x)+xv(x)\in(2,x)=\left\{2p_1(x)+xp_2(x)\,\middle|\,p_i(x)\in R[x]\right\},$$

即 $1\in(2,x)$. 所以$(2,x)=(1)$.

证二 因 $R[x]$是有单位元的交换环,故

$$(2,x)=\left\{2p_1(x)+xp_2(x)\,\middle|\,p_i(x)\in R[x]\right\}.$$

而 $1=2\cdot\frac{1}{2}+x\cdot 0$,其中$\frac{1}{2},0\in R[x]$,因此 $1\in(2,x)$.

所以$(2,x)=(1)$.

证三 因 $R[x]$是有单位元的交换环,故

$$(2,x)=\left\{2p_1(x)+xp_2(x)\,\middle|\,p_i(x)\in R[x]\right\}.$$

从而$\forall\, a_0+a_1x+a_2x^2+\cdots+a_nx^n\in R[x]$,有

$$a_0+a_1x+a_2x^2+\cdots+a_nx^n=2\cdot\frac{a_0}{2}+x(a_1+a_2x+\cdots+a_nx^{n-1})\in(2,x).$$

因此 $R[x]\subset(2,x)$,显然$(2,x)\subset R[x]$. 因 $1\in R[x]$,故 $R[x]=(1)$. 所以$(2,x)=R[x]=(1)$.

注 1) 设 R 是任一数域,都有$(2,x)=(1)$.

2) 在证一中,若 R 是整数环,虽 $2,x$ 互素,却不存在 $u(x),v(x)\in R[x]$,使得 $2u(x)+xv(x)=1$.

3) 若 R 是整数环,已知$(2,x)$不是 $R[x]$的一个主理想. 一般来说,若 $R(\neq\{0\})$是有单位元的交换环而不是域,则(a,x)不是 $R[x]$的主理想,其中 $a(\neq 0)$不是 R 的可逆元.

事实上,因 $R(\neq\{0\})$不是域,故∃$a(\neq 0)\in R$,a 不是 R 的可逆元. 因 $R[x]$是有单位元的交换环,故

$$(a,x)=\left\{ap_1(x)+xp_2(x)\,\middle|\,p_i(x)\in R[x]\right\}$$
$$=\left\{a(b_0+b_1x+\cdots+b_sx^s)+x(c_0+c_1x+\cdots+c_tx^t)\,\middle|\,b_i,c_j\in R,s,t\text{ 是非负整数}\right\}$$
$$=\left\{ab_0+a_1x+\cdots+a_nx^n\,\middle|\,b_0,a_i\in R,n\text{ 是非负整数}\right\}.$$

则(a,x)不是$R[x]$的主理想. 不然,假设$(a,x)=(p(x))$,则$a\in(p(x))$,即$a=p(x)k(x)$. 因x是未定元,故$p(x)=b\in R$. 且$x\in(p(x))$,即$x=p(x)h(x)=bh(x)$. 因x是未定元,故$h(x)$只能是一次多项式. 设$h(x)=h_0+h_1x$,其中$h_0,h_1\in R$,于是$x=b(h_0+h_1x)=bh_0+bh_1x$. 因x是未定元,故$bh_1=1$,从而$p(x)=b$是$R[x]$的可逆元,即$(a,x)=(b)$. 因$b\in(a,x)$,故$\exists\, a_0\in R$,使得$aa_0=b$,因b是可逆元,故$a(a_0b^{-1})=1$,其中$a_0b^{-1}\in R$,于是a是可逆元,发生矛盾.(证明了$p(x)=b$是$R[x]$的可逆元以后,还可如下推理:由第十二章,一,4,9),$(p(x))=R[x]=(1)$,即$(a,x)=R[x]$. $1\in R[x]$,但$1\overline{\in}(a,x)$,否则,若$1\in(a,x)$,则$\exists\, c\in R$,使得$ac=1$,于是a可逆,矛盾.)所以(a,x)不是$R[x]$的主理想.

4. 证明:两个理想的交集还是一个理想.

证 设$\mathfrak{A},\mathfrak{B}$是环$R$的两个理想. 因理想是子环,故$0\in\mathfrak{A},0\in\mathfrak{B}$,从而$0\in\mathfrak{A}\cap\mathfrak{B}$,即$\mathfrak{A}\cap\mathfrak{B}\neq\varnothing$. 显然$\mathfrak{A}\cap\mathfrak{B}\subset R$. $\forall\, a,b\in\mathfrak{A}\cap\mathfrak{B}$,有$a,b\in\mathfrak{A}$且$a,b\in\mathfrak{B}$. 因$\mathfrak{A},\mathfrak{B}$是环,故$a-b\in\mathfrak{A}$且$a-b\in\mathfrak{B}$,于是$a-b\in\mathfrak{A}\cap\mathfrak{B}$. $\forall\, a\in\mathfrak{A}\cap\mathfrak{B},\forall\, r\in R$,有$a\in\mathfrak{A}$且$a\in\mathfrak{B}$,因$\mathfrak{A},\mathfrak{B}$是理想,故$ra,ar\in\mathfrak{A}$且$ra,ar\in\mathfrak{B}$,因此$ra,ar\in\mathfrak{A}\cap\mathfrak{B}$. 所以$\mathfrak{A}\cap\mathfrak{B}$是$R$的一个理想.

注 1) 设$(a),(b)$是整数环$\mathbb{Z}$的两个主理想,则

$$(a)\cap(b)=(m)\Leftrightarrow m\text{ 是 }a,b\text{ 的一个最小公倍数}.$$

事实上,($\Rightarrow$) 因$m\in(a)\cap(b)$,故$m\in(a)$且$m\in(b)$,从而$\exists\, s,t\in\mathbb{Z}$,使得$m=as$,$m=bt$,即$a\mid m$且$b\mid m$. 设$k$是$a,b$的任一公倍数,则$k\in(a)$且$k\in(b)$,即$k\in(a)\cap(b)=(m)$,从而$m\mid k$. 所以$m$是$a,b$的一个最小公倍数.($\Leftarrow$) 因$m$是$a,b$的一个最小公倍数,故$a\mid m$且$b\mid m$,从而$\exists\, u,v\in\mathbb{Z}$,使得$m=au,m=bv$,即$m\in(a)$且$m\in(b)$,于是$(m)\subset(a)$且$(m)\subset(b)$,因此$(m)\subset(a)\cap(b)$;反之,$\forall\, c\in(a)\cap(b)$,有$c\in(a)$且$c\in(b)$,从而$\exists\, i,j\in\mathbb{Z}$,使得$c=ai,c=bj$,于是$a\mid c,b\mid c$. 因$m$是$a,b$的一个最小公倍数,故$m\mid c$,即$\exists\, q\in\mathbb{Z}$,使得$c=mq$,因此$c\in(m)$,可见$(a)\cap(b)\subset(m)$. 所以$(a)\cap(b)=(m)$.

2) 设$\mathfrak{A},\mathfrak{B}$是环$R$的理想,则$\left\{a+b\,\middle|\,a\in\mathfrak{A},b\in\mathfrak{B}\right\}$是包含$\mathfrak{A}$与$\mathfrak{B}$的$R$的最小理想,称之为$\mathfrak{A}$与$\mathfrak{B}$的和,记为$\mathfrak{A}+\mathfrak{B}$(见第八章,二,4,注 10)).

事实上,因$0+0=0\in\mathfrak{A}+\mathfrak{B}$,故$\mathfrak{A}+\mathfrak{B}\neq\varnothing$. 显然$\mathfrak{A}+\mathfrak{B}\subset R$. $\forall\, x=a+b,y=a'+b'\in\mathfrak{A}+\mathfrak{B}$,其中$a,a'\in\mathfrak{A},b,b'\in\mathfrak{B}$,因$\mathfrak{A},\mathfrak{B}$是理想,故$a-a'\in\mathfrak{A},b-b'\in\mathfrak{B}$,从而

$$x-y=(a+b)-(a'+b')=a+b+[(-a')+(-b')]=[a+(-a')]+[b+(-b')]$$
$$=(a-a')+(b-b')\in\mathfrak{A}+\mathfrak{B}.$$

$\forall\, x=a+b\in\mathfrak{A}+\mathfrak{B},\forall\, r\in R$,其中$a\in\mathfrak{A},b\in\mathfrak{B}$. 因$\mathfrak{A},\mathfrak{B}$是理想,故$ra,ar\in\mathfrak{A},rb,br\in\mathfrak{B}$,从而

$$rx=r(a+b)=ra+rb\in\mathfrak{A}+\mathfrak{B},\quad xr=(a+b)r=ar+br\in\mathfrak{A}+\mathfrak{B},$$

所以$\mathfrak{A}+\mathfrak{B}$是$R$的理想.

$\forall\, a\in\mathfrak{A},a=a+0\in\mathfrak{A}+\mathfrak{B}$,其中$0\in\mathfrak{B}$,从而$\mathfrak{A}\subset\mathfrak{A}+\mathfrak{B}$. 同理$\mathfrak{B}\subset\mathfrak{A}+\mathfrak{B}$.

设I是R的含$\mathfrak{A}$与$\mathfrak{B}$的理想. $\forall\, x=a+b\in\mathfrak{A}+\mathfrak{B}$,其中$a\in\mathfrak{A},b\in\mathfrak{B}$,从而$a,b\in I$. 因$I$是

理想，故 $x=a+b\in I$，于是$\mathfrak{A}+\mathfrak{B}\subset I$.

所以$\mathfrak{A}+\mathfrak{B}$是含$\mathfrak{A}$与$\mathfrak{B}$的 R 的最小理想.

3)　设 S,T 是环 R 的左(右)理想(见第十二章，二，6)，则$\{a+b\mid a\in S,b\in T\}$是 R 的一个左(右)理想，称之为 S 与 T 的和，记为 $S+T$.

请读者自证.

4)　设(a)，(b)是整数环$\mathbb{Z}$的两个主理想，则

$$(a)+(b)=(d)\Leftrightarrow d\text{ 是 }a,b\text{ 的一个最大公因子.}$$

事实上，($\Rightarrow$)　因 $a\in(a)+(b)=(d)$，故 $\exists q\in\mathbb{Z}$，使得 $a=dq$，即 $d\mid a$. 同理 $d\mid b$. 又 $d\in(a)+(b)$，从而 $\exists u,v\in\mathbb{Z}$，使得 $d=au+bv$. 所以 d 是 a,b 的一个最大公因子. ($\Leftarrow$)　因 d 是 a,b 的一个最大公因子，故 $d\mid a,d\mid b$，从而 $a\in(d)$，$b\in(d)$，于是$(a)\subset(d)$，$(b)\subset(d)$，又(d) 是环，因此$(a)+(b)\subset(d)$；反之，因 d 是 a,b 的一个最大公因子，故 $\exists s,t\in\mathbb{Z}$，使得 $d=as+bt$，从而 $d\in(a)+(b)$，因此$(d)\subset(a)+(b)$. 所以$(a)+(b)=(d)$.

5)　设(a)，(b)是$\mathbb{Z}$的两个主理想，则

$$(a)+(b)=(a,b).$$

事实上，显然$(a)\subset(a,b)$，$(b)\subset(a,b)$，而(a,b)是环，因此$(a)+(b)\subset(a,b)$；反之，$\forall x\in(a,b)$，$\exists u,v\in\mathbb{Z}$，$x=au+bv\in(a)+(b)$，从而$(a,b)\subset(a)+(b)$. 所以$(a)+(b)=(a,b)$.

该命题可推广为：设$(a_1,a_2,\cdots,a_n)$，$(b_1,b_2,\cdots,b_m)$是$\mathbb{Z}$的两个理想，则

$$(a_1,a_2,\cdots,a_n)+(b_1,b_2,\cdots,b_m)=(a_1,a_2,\cdots,a_n,b_1,b_2,\cdots,b_m).$$

6)　任意多个理想的交集与和集还是理想.

请读者自证.

7)　环 R 的两个理想的并未必是 R 的理想. 例，$2\mathbb{Z}$ 与 $3\mathbb{Z}$ 都是整数环 $\mathbb{Z}$ 的理想. 因 $2,3\in 2\mathbb{Z}\cup 3\mathbb{Z}$，但 $2+3=5\,\overline{\in}\,2\mathbb{Z}\cup 3\mathbb{Z}$，故 $2\mathbb{Z}\cup 3\mathbb{Z}$ 不是 $\mathbb{Z}$ 的理想.

8)　设$\mathfrak{A}$，$\mathfrak{B}$是环 R 的理想，集 $S=\{ab\mid a\in\mathfrak{A},b\in\mathfrak{B}\}$ 未必是 R 的理想. 例，取$\mathfrak{A}=(x,y)$，$\mathfrak{B}=(x^2,y)$，则$\mathfrak{A}$，$\mathfrak{B}$是环$\mathbb{Z}[x,y]$的理想. 因 $x^3=x\cdot x^2\in S$，$y^2=y\cdot y\in S$，但 x^3+y^2 写不成形式：ab，$a\in\mathfrak{A}$，$b\in\mathfrak{B}$，即 $x^3+y^2\,\overline{\in}\,S$. 故 S 不是 R 的理想. 正是因为两个乘积 ab 与 $a'b'$的和不一定能表成乘积 cd，其中 $c\in\mathfrak{A}$，$d\in\mathfrak{B}$，我们将集合扩大一些，得出下面命题.

9)　设$\mathfrak{A}$，$\mathfrak{B}$是环 R 的理想，则

$$\left\{\text{一切有限和}\sum_{i=1}^{n}x_iy_i\,\middle|\,x_i\in\mathfrak{A},y_i\in\mathfrak{B},n\text{ 是正整数}\right\}$$

是 R 的一个理想. 称之为$\mathfrak{A}$与$\mathfrak{B}$的积，记为$\mathfrak{A}\mathfrak{B}$.

事实上，因 $0\cdot 0=0\in\mathfrak{A}\mathfrak{B}$，故$\mathfrak{A}\mathfrak{B}\neq\varnothing$. 显然$\mathfrak{A}\mathfrak{B}\subset R$. $\forall\sum x_iy_i,\sum x'_iy'_i\in\mathfrak{A}\mathfrak{B}$，

$$\sum x_iy_i-\sum x'_iy'_i=\sum x_iy_i+\sum(-x'_i)y'_i$$

仍是有限和，从而$\sum x_iy_i-\sum x'_iy'_i\in\mathfrak{A}\mathfrak{B}$. $\forall\sum x_iy_i\in\mathfrak{A}\mathfrak{B}$，$\forall r\in R$，因$\mathfrak{A}$，$\mathfrak{B}$是理想，故

$$r(\sum x_iy_i)=\sum(rx_i)y_i\in\mathfrak{A}\mathfrak{B},\ (\sum x_iy_i)r=\sum x_i(y_ir)\in\mathfrak{A}\mathfrak{B}.$$

所以$\mathfrak{A}\mathfrak{B}$是 R 的理想.

10)　设 S,T 是环 R 的左(右)理想，则$\{\sum a_ib_i\mid a_i\in S,\ b_i\in T\}$是 R 的一个左(右)理

想，称之为 S 与 T 的积，记为 ST.

请读者自证.

11） 设 S 与 T 分别是环 R 的左理想与右理想，则 $\left\{\sum a_i b_i \,\middle|\, a_i \in S, b_i \in T\right\}$ 是 R 的一个理想，记为 ST.

请读者自证.

12） 设 $(a),(b)$ 是 $\mathbb{Z}$ 的两个主理想，则

$$(a)(b)=(ab).$$

事实上，$\forall x \in (a)(b)$，$\exists s_i, t_i \in \mathbb{Z}$，使得 $x=\sum (s_i a)(t_i b)=(\sum s_i t_i)ab \in (ab)$，所以 $(a)(b) \subset (ab)$；反之，$\forall x \in (ab)$，$\exists u \in \mathbb{Z}$，使得 $x=u(ab)=(ua)b \in (a)(b)$，所以 $(ab) \subset (a)(b)$. 于是 $(a)(b)=(ab)$.

该命题可推广为：设 $(a_1, a_2, \cdots, a_n)$，$(b_1, b_2, \cdots, b_m)$ 是 $\mathbb{Z}$ 的两个理想，则

$$(a_1, a_2 \cdots, a_n)(b_1, b_2, \cdots, b_m)=(a_1 b_1, \cdots, a_1 b_m, \cdots, a_n b_1, \cdots, a_n b_m).$$

13） 设 $(a),(b)$ 是 $\mathbb{Z}$ 的两个主理想，则

$$(a)(b)=(a) \cap (b) \Leftrightarrow a, b \text{ 互素}.$$

事实上，（$\Rightarrow$） 由 $(a)(b)=(a)\cap(b)$，有 $(ab)=(m)$，其中 m 是 a,b 的最小公倍数，从而 $ab \mid m$，$m \mid ab$，于是 $|ab|=m$. 设 d 是 a,b 的最大公因数，则 $|ab|=md$，从而 $d=1$. 因此 a,b 互素.（$\Leftarrow$） 设 d 是 a,b 的最大公因数，m 是 a,b 的最小公倍数，则 $|ab|=md$. 今已知 $d=1$，从而 $|ab|=m$. 所以 $(ab)=(m)$，即 $(a)(b)=(a)\cap(b)$.

例 1 (12)，(21)是 $\mathbb{Z}$ 的两个主理想. 因 84 是 12 与 21 的最小公倍数，3 是 12 与 21 的最大公因数，故 $(12)\cap(21)=(84)$. $(12)+(21)=(3)$. $(12)(21)=(12\times 21)=(252)$.

例 2 设 p,q 是两个素数，当 $p=q$ 时，$(p)\cap(q)=(p)$，$(p)+(q)=(p)$. $(p)(q)=(p^2)$. 当 $p\neq q$ 时，$(p)\cap(q)=(pq)$，$(p)+(q)=(1)$，$(p)(q)=(pq)$.

14） 设 $\mathfrak{A},\mathfrak{B}$ 是环 R 的理想，则 $\mathfrak{A}$ 是环 $\mathfrak{A}+\mathfrak{B}$ 的理想（见第十二章，一，5，4），注②，例 3）.

事实上，因 $\mathfrak{A}$ 是 R 的理想，故 $\mathfrak{A}$ 是加群 $\mathfrak{A}+\mathfrak{B}$ 的子加群. $\forall a \in \mathfrak{A}$，$\forall r \in \mathfrak{A}+\mathfrak{B} \subset R$，因 $\mathfrak{A}$ 是 R 的理想，故 $ra, ar \in \mathfrak{A}$. 所以 $\mathfrak{A}$ 是环 $\mathfrak{A}+\mathfrak{B}$ 的理想.

可将该命题推广如下：设 $\mathfrak{A}$ 是环 R 的理想，S 是 R 的子环且 $\mathfrak{A} \subset S \subset R$，则 $\mathfrak{A}$ 是环 S 的理想（见第八章，三，2，5））.

15） 设 $\mathfrak{A}$ 是环 R 的理想，S 是 R 的子环，则 $\mathfrak{A}\cap S$ 是 S 的理想（见第十二章，一，5，4），注②，例 4）.

事实上，因 $\mathfrak{A}\cap S$ 是 R 的子环，故 $\mathfrak{A}\cap S \neq \varnothing$. 显然 $\mathfrak{A}\cap S \subset S$. $\forall a, b \in \mathfrak{A}\cap S$，有 $a,b \in \mathfrak{A}$ 且 $a,b \in S$. 因 $\mathfrak{A}$ 与 S 都是环，故 $a-b \in \mathfrak{A}$ 且 $a-b \in S$，从而 $a-b \in \mathfrak{A}\cap S$. $\forall a \in \mathfrak{A}\cap S$，$s \in S$，有 $a \in \mathfrak{A}$ 且 $a \in S$. 因 $\mathfrak{A}$ 是 R 的理想，S 是 R 的子环，故 $sa \in \mathfrak{A}$ 且 $sa \in S$，从而 $sa \in \mathfrak{A}\cap S$. 同理 $as \in \mathfrak{A}\cap S$. 所以 $\mathfrak{A}\cap S$ 是 S 的理想.

5. 找出模 6 的剩余类环 $\mathbb{Z}_6$ 的所有理想.

解 环 $\mathbb{Z}_6$ 的理想是加群 $\mathbb{Z}_6$ 的子加群，则 $\mathbb{Z}_6$ 是循环加群①. 由第七章，二，3，$\mathbb{Z}_6$ 的子加群

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 57. 例 2.

是循环加群. 从而$\mathbb{Z}_6$的全部子加群是以下4个：

$$([0])=\{[0]\},\qquad ([1])=\mathbb{Z}_6=([5]),$$

$$([2])=\{[0],[2],[4]\}=([4]),\quad ([3])=\{[0],[3]\}.$$

显然$([0])$,$([1])$是$\mathbb{Z}_6$的理想. 又

$$([2])=\{q[2]\mid q\in\mathbb{Z}\}=\{[q][2]\mid [q]\in\mathbb{Z}_6\}.$$

$$([3])=\{q[3]\mid q\in\mathbb{Z}\}=\{[q][3]\mid [q]\in\mathbb{Z}_6\}.$$

因$\mathbb{Z}_6$是有单位元的交换环，故$([2])$与$([3])$分别是$\mathbb{Z}_6$的由$[2]$与$[3]$生成的主理想. 所以$([0])$,$([1])$,$([2])$,$([3])$是$\mathbb{Z}_6$的所有理想.

注　1)　一般来说，加群$\mathbb{Z}_n$的循环子加群$([a])$必为环$\mathbb{Z}_n$的主理想. 事实上，$\mathbb{Z}_n$的子加群

$$([a])=\{q[a]\mid q\in\mathbb{Z}\}=\{[qa]\mid q\in\mathbb{Z}\}=\{[q][a]\mid [q]\in\mathbb{Z}_n\}.$$

因为$\mathbb{Z}_n$是有单位元的交换环，所以加群$\mathbb{Z}_n$的由$[a]$生成的循环子加群$([a])$就是环$\mathbb{Z}_n$的由$[a]$生成的主理想.

由此可知，$\mathbb{Z}_n$的每一理想都是主理想.

若将$\mathbb{Z}_n$改成为一般的有单位元的交换环，结论不对(见第十二章，一，4，13)).

2)　环$\mathbb{Z}_n$的理想的个数等于n的正因子的个数. 事实上，由第七章，一，10，因$\mathbb{Z}_n$是有限n阶循环加群，故$\forall$正整数m且$m\mid n$，$\mathbb{Z}_n$有m阶子群. 再由第七章，三，2，1)，$\mathbb{Z}_n$存在且只存在一个阶为m的子加群，即$\mathbb{Z}_n$的子加群的个数等于n的正因子的个数，由本注1)知，环$\mathbb{Z}_n$的理想的个数等于n的正因子的个数.

例　12的正因子是：1，2，3，4，6，12，共有6个. 从而$\mathbb{Z}_{12}$有6个理想：

$$([0])=\{[0]\},$$

$$([1])=\mathbb{Z}_{12}=([5])=([7])=([11]),$$

$$([2])=\{[0],[2],[4],[6],[8],[10]\}=([10]),$$

$$([3])=\{[0],[3],[6],[9]\}=([9]),$$

$$([4])=\{[0],[4],[8]\}=([8]),$$

$$([6])=\{[0],[6]\}=([6]).$$

3)　因$\mathbb{Z}_6$有且只有4个理想，故由同态基本定理，$\mathbb{Z}_6$的所有的模理想的剩余类环为以下4个：

$$\mathbb{Z}_6/([0])=\{\{[a]\}\mid [a]\in\mathbb{Z}_6\}\cong\mathbb{Z}_6.$$

$\mathbb{Z}_6/([1])=\mathbb{Z}_6/\mathbb{Z}_6=\{([1])\}=\{[[0]]\}$，其中$[[0]]$是$\mathbb{Z}_6/([1])$的零元.

$$\mathbb{Z}_6/([2])=\{[a]+([2])\mid [a]\in\mathbb{Z}_6\}=\{\{[0],[2],[4]\},\{[1],[3],[5]\}\}.$$

$$\mathbb{Z}_6/([3])=\{[a]+([3])\mid [a]\in\mathbb{Z}_6\}=\{\{[0],[3]\},\{[1],[4]\},\{[2],[5]\}\}.$$

6. 一个环R的一个非空子集S叫做R的一个左理想，假如

(i)　$a,b\in S\Rightarrow a-b\in S$,

(ii)　$a\in S, r\in R\Rightarrow ra\in S$.

你能不能在有理数域$\mathbb{Q}$上的2×2矩阵环$M_2(\mathbb{Q})$里找到一个不是理想的左理想？

解 取 $S=\left\{\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \middle| x,y\in\mathbb{Q}\right\}$. 显然 $S\subset M_2(\mathbb{Q})$. 因 $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\in S$，故 $S\neq\varnothing$. $\forall \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix},\begin{pmatrix} u & 0 \\ v & 0 \end{pmatrix}\in S$，

$$\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix}-\begin{pmatrix} u & 0 \\ v & 0 \end{pmatrix}=\begin{pmatrix} x-u & 0 \\ y-v & 0 \end{pmatrix}\in S.$$

$\forall \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix}\in S$，$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in M_2(\mathbb{Q})$，

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix}=\begin{pmatrix} ax+by & 0 \\ cx+dy & 0 \end{pmatrix}\in S.$$

所以 S 是 $M_2(\mathbb{Q})$的一个左理想.

取$\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix}\in S$，$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in M_2(\mathbb{Q})$，而其中 $xb\neq 0$ 或 $yb\neq 0$，因

$$\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} xa & xb \\ ya & yb \end{pmatrix}\overline{\in} S,$$

故 S 不是 $M_2(\mathbb{Q})$的理想.

取 $S=\left\{\begin{pmatrix} 0 & x \\ 0 & y \end{pmatrix} \middle| x,y\in\mathbb{Q}\right\}$或取 $S=\left\{\begin{pmatrix} x & x \\ y & y \end{pmatrix} \middle| x,y\in\mathbb{Q}\right\}$，它们都是 $M_2(\mathbb{Q})$的左理想，但不是理想.

注 1) 环 R 的一个非空子集 S 叫做 R 的一个右理想，假如

(i) $a,b\in S\Rightarrow a-b\in S$，

(ii) $a\in S,r\in R\Rightarrow ar\in S$.

$$\left\{\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \middle| x,y\in\mathbb{Q}\right\},\ \left\{\begin{pmatrix} 0 & 0 \\ x & y \end{pmatrix} \middle| x,y\in\mathbb{Q}\right\},\ \left\{\begin{pmatrix} x & y \\ x & y \end{pmatrix} \middle| x,y\in\mathbb{Q}\right\}$$

都是 $M_2(\mathbb{Q})$的右理想，但不是理想.

2) 设 F 是域，I_k 是环 $M_n(F)(n\geqslant 2)$中只可能在第 k 列有非零元的 n 阶矩阵的集，则 I_k 是 $M_n(F)$的左理想，但不是右理想. 设 J_k 是环 $M_n(F)(n\geqslant 2)$中只可能在第 k 行有非零元的 n 阶矩阵的集，则 J_k 是 $M_n(F)$的右理想，但不是左理想.

3) 设 R 是环，R 有不是零元的非零因子，则

$$S=\left\{\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1k} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2k} & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nk} & 0 & \cdots & 0 \end{pmatrix} \middle| a_{ij}\in R\right\}$$

是 $M_n(R)(n\geqslant 2)$的一个左理想. R 上的下方 $n-k$ 行都是 0 的 n 阶矩阵的集 T 是 $M_n(R)$ $(n\geqslant 2)$的一个右理想. S 与 T 都不是理想.

4) 设 R 是环，取定 $a\in R$. 则

$$Ra=\left\{ra \middle| r\in R\right\} \text{ 和 } aR=\left\{ar \middle| r\in R\right\}$$

分别是 R 的左理想和右理想. 如果 R 有单位元，那么 $a\in Ra, a\in aR$. 且 $Ra(aR)$ 是含 a 的最小左(右)理想. 如果 R 无单位元，那么 $\{ra+na \mid r\in R, n\in \mathbb{Z}\}$ ($\{ar+na \mid r\in R, n\in \mathbb{Z}\}$) 是含 a 的最小左(右)理想，称为由 a 生成的主左(右)理想.

7. 假定我们有一个环 R 的一个分类，而 S 是由所有的类 $[a],[b],[c],\cdots$ 所成的集合. 又假定

$$[x]+[y]=[x+y],\quad [x][y]=[xy].$$

规定两个 S 的代数运算，证明：$[0]$ 是 R 的一个理想，并且给定的类刚好是模 $[o]$ 的 R 的剩余类.

证一　1)　因 $0\in[0]$，故 $[0]\neq\varnothing$. 显然 $[0]\subset R$. $\forall x,y\in[0]$，有 $[x]=[y]=[0]$，从而

$$[x-y]=[x+(-y)]=[x]+[-y]=[y]+[-y]=[y+(-y)]=[0].$$

于是 $x-y\in[0]$. $\forall r\in R, \forall x\in[0]$，有 $[x]=[0]$，从而

$$[rx]=[r][x]=[r][0]=[r0]=[0].$$

于是 $rx\in[0]$. 同理 $xr\in[0]$. 所以 $[0]$ 是 R 的一个理想.

2)　$\forall [a]\in S$，往证 $[a]$ 是模 $[0]$ 的 R 的剩余类.

①　$\forall x,y$ 属于 S 中的同一个类 $[a]$. 因 $[x]=[y]=[a]$，故

$$[x-y]=[x+(-y)]=[x]+[-y]=[y]+[-y]=[y+(-y)]=[0],$$

从而 $x-y\in[0]$. 所以 x,y 属于模 $[0]$ 的同一个剩余类.

②　$\forall x,y$ 属于模 $[0]$ 的同一个剩余类. 即 $x-y\in[0]$，从而 $[x-y]=[0]$，于是

$$\begin{aligned}[x]&=[x+0]=[x+((-y)+y)]=[(x-y)+y]=[x-y]+[y]\\&=[0]+[y]=[0+y]=[y].\end{aligned}$$

所以 x,y 属于 S 中的同一个类.

综上可知，$\forall [a]\in S$，$[a]$ 是模 $[0]$ 的 R 的剩余类.

证二　1)　见证一.

2)　$\forall [a]\in S$，往证 $[a]=\{a+u \mid u\in[0]\}$. $\forall x\in[a]$，有 $[x]=[a]$. 令 $u'=x-a\in R$，则 $x=a+u'$，下面证明 $u'\in[0]$. 因

$$[u']=[x-a]=[x+(-a)]=[x]+[-a]=[a]+[-a]=[a+(-a)]=[0],$$

故 $u'\in[0]$，从而 $x=a+u'\in\{a+u \mid u\in[0]\}$. 于是 $[a]\subset\{a+u \mid u\in[0]\}$. 另一方面，$\forall a+u\in\{a+u \mid u\in[0]\}$，因 $[u]=[0]$，故

$$[a+u]=[a]+[u]=[a]+[0]=[a+0]=[0],$$

从而 $a+u\in[a]$. 于是 $\{a+u \mid u\in[0]\}\subset[a]$. 因此，$[a]=\{a+u \mid u\in[0]\}$，所以，$\forall [a]\in S$，$[a]$ 是模 $[0]$ 的 R 的剩余类.

注　$S=R/[0]$.

8. 假定 ϕ 是环 R 到环 $\overline{R}$ 的一个同态满射. 证明：ϕ 是 R 与 $\overline{R}$ 间的同构映射，当且只当 ϕ 的核是 R 的零理想的时候.

证一　因 ϕ 是 R 与 $\overline{R}$ 间的同构映射，故 ϕ 是单射，即 $\overline{R}$ 的零元 $\overline{0}$ 在 ϕ 下的逆象唯一，有且只有 R 中的零元 0，从而 $\ker\phi=\{0\}$.

$\forall a,b\in R$，若 $\phi(a)=\phi(b)$，则 $\phi(a-b)=\phi(a)-\phi(b)=\overline{0}$，从而 $a-b\in\ker\phi=\{0\}$. 于

是 $a-b=0$，即 $a=b$. 因此ϕ是单射. 再结合已知条件，知ϕ是 R 与 $\overline{R}$ 间的同构映射.

证二 必要性的证明见证一. 下面证明充分性. 因 $\ker\phi=\{0\}$，故 $R/\ker\phi=R/\{0\}\cong R$. 由同态基本定理，$R/\ker\phi\cong\overline{R}$. 再由同构的对称性和传递性，$R\cong\overline{R}$. 且这个$\phi$就是 R 与 $\overline{R}$ 间的同构映射.

注 因ϕ是环 R 到环 $\overline{R}$ 的一个同态满射，当然ϕ就是加群 R 到加群 $\overline{R}$ 的一个同态满射. 由第八章，三，13 知：

$$\phi\text{是单射}\Leftrightarrow \ker\phi=\{0\},$$

从而命题得证.

9. 假定 R 是由所有复数 $a+b\mathrm{i}$（a,b 是整数）作成的环. 环 $R/(1+\mathrm{i})$ 有多少元?

解一 先弄清核心部分 $(1+\mathrm{i})$ 由哪些元组成. 实际上，

$$(1+\mathrm{i})=\left\{a+b\mathrm{i}\,\middle|\,a,b\in\mathbb{Z},a,b\text{ 同奇偶}\right\},$$

这是因为：$\forall a+b\mathrm{i}\in(1+\mathrm{i})$. 因 R 是有单位元的交换环，故

$$a+b\mathrm{i}=(x+y\mathrm{i})(1+\mathrm{i})=(x-y)+(x+y)\mathrm{i},$$

其中 $x,y\in\mathbb{Z}$，从而 $a=x-y$，$b=x+y$. 当 x,y 同奇或同偶时，a,b 同偶；当 x,y 一奇一偶时，a,b 同奇. 因此无论 x,y 是什么整数时，a,b 总是同奇偶. 于是 $a+b\mathrm{i}\in\left\{a+b\mathrm{i}\,\middle|\,a,b\in\mathbb{Z},a,b\text{ 同奇偶}\right\}$，即 $(1+\mathrm{i})\subset\left\{a+b\mathrm{i}\,\middle|\,a,b\in\mathbb{Z},a,b\text{ 同奇偶}\right\}$. 反之，$\forall a+b\mathrm{i}\in\left\{a+b\mathrm{i}\,\middle|\,a,b\in\mathbb{Z},a,b\text{ 同奇偶}\right\}$. 因 a,b 同奇偶，故方程组

$$\begin{cases}x-y=a,\\x+y=b\end{cases}$$

有整数解 $x=\frac{a+b}{2}$，$y=\frac{b-a}{2}$，从而 $\exists x+y\mathrm{i}\in R$，其中 $x,y\in\mathbb{Z}$，使得

$$a+b\mathrm{i}=(x-y)+(x+y)\mathrm{i}=(x+y\mathrm{i})(1+\mathrm{i}),$$

因此 $a+b\mathrm{i}\in(1+\mathrm{i})$. 于是 $\left\{a+b\mathrm{i}\,\middle|\,a,b\in\mathbb{Z},a,b\text{ 同奇偶}\right\}\subset(1+\mathrm{i})$. 所以 $(1+\mathrm{i})=\left\{a+b\mathrm{i}\,\middle|\,a,b\in\mathbb{Z},a,b\text{ 同奇偶}\right\}$. $\forall a+b\mathrm{i}\in R$，当 a,b 同奇偶时，$a+b\mathrm{i}\in(1+\mathrm{i})$，即 $[a+b\mathrm{i}]=(1+\mathrm{i})=[0]$；当 a,b 一奇一偶时，$a-1$ 与 b 有相同的奇偶性，从而

$$a+b\mathrm{i}=1+[(a-1)+b\mathrm{i}]\in 1+(1+\mathrm{i}),$$

即 $[a+b\mathrm{i}]=1+(1+\mathrm{i})=[1]$. 所以 $R/(1+\mathrm{i})=\{[0],[1]\}$.

解二 作集合 $\overline{R}=\{0,1\}$，规定运算

+	0	1
0	0	1
1	1	0

•	0	1
0	0	0
1	0	1

于是 $\overline{R}$ 作成一个环. 规定：$\forall a+b\mathrm{i}\in R$，当 $a+b\mathrm{i}\in(1+\mathrm{i})$ 时，

$$\phi:a+b\mathrm{i}\to 0.$$

当 $a+b\mathrm{i}\in R-(1+\mathrm{i})$ 时

$$\phi:a+b\mathrm{i}\to 1.$$

则ϕ是 R 到 $\overline{R}$ 的一个同态满射. 事实上，

1)　$\forall a+bi\in R$ 在ϕ下有且只有一个象$\in\overline{R}$.

2)　因$(1+\mathrm{i})$是 R 的主理想,故$(1+\mathrm{i})$不空,从而 $0(\in\overline{R})$在ϕ下有逆象.因

$$(1+\mathrm{i})=\left\{a+bi\,\middle|\,a,b\in\mathbb{Z}\ ,a,b\text{ 同奇偶}\right\}.$$

(见解一)故

$$R-(1+\mathrm{i})=\left\{a+bi\,\middle|\,a,b\in\mathbb{Z}\ ,a,b\text{ 不同奇偶}\right\}$$

不空,从而 $1(\in\overline{R})$在ϕ下有逆象.

3)　①　$\forall a+bi,c+di\in(1+\mathrm{i}),\phi(a+bi)=0,\phi(c+di)=0$. 因$(1+\mathrm{i})$是环,故$(a+bi)+(c+di)\in(1+\mathrm{i}),(a+bi)(c+di)\in(1+\mathrm{i})$,从而$\phi[(a+bi)+(c+di)]=0=0+0=\phi(a+bi)+\phi(c+di),\phi[(a+bi)(c+di)]=0=0\cdot 0=\phi(a+bi)\cdot\phi(c+di)$.

②　$\forall a+bi,c+di\in R-(1+\mathrm{i}),\phi(a+bi)=1,\phi(c+di)=1$. 此时易证$(a+bi)+(c+di)\in(1+\mathrm{i})$,而$(a+bi)(c+di)\in R-(1+\mathrm{i})$,因此$\phi[(a+bi)+(c+di)]=0=1+1=\phi(a+bi)+\phi(c+di),\phi[(a+bi)(c+di)]=1=1\cdot 1=\phi(a+bi)\cdot\phi(c+di)$.

③　$\forall a+bi\in(1+\mathrm{i}),c+di\in R-(1+\mathrm{i}),\phi(a+bi)=0,\phi(c+di)=1$. 显然$(a+bi)+(c+di)\in R-(1+\mathrm{i})$. 因$(1+\mathrm{i})$是理想,故$(a+bi)(c+di)\in(1+\mathrm{i})$,从而$\phi[(a+bi)+(c+di)]=1=0+1=\phi(a+bi)+\phi(c+di),\phi[(a+bi)(c+di)]=0=0\cdot 1=\phi(a+bi)\cdot\phi(c+di)$. 又 R 是交换环,所以 $R\overset{\phi}{\sim}\overline{R}$. 显然 $\ker\phi=(1+\mathrm{i})$. 由同态基本定理,$R/(1+\mathrm{i})\cong\overline{R}$. 因 $\overline{R}$ 有两个元,故 $R/(1+\mathrm{i})$也有两个元.

解三　取$[0],[1]\in R/(1+\mathrm{i})$,于是

$$[0]=\left\{0+u\,\middle|\,u\in(1+\mathrm{i})\right\}=(1+\mathrm{i})=\left\{a+bi\,\middle|\,a,b\in\mathbb{Z}\ ,a,b\text{ 同奇偶}\right\},$$

$$[1]=\left\{1+u\,\middle|\,u\in(1+\mathrm{i})\right\}=\left\{1+(1+\mathrm{i})(x+y\mathrm{i})\,\middle|\,x,y\in\mathbb{Z}\right\}$$

$$=\left\{(1+x-y)+(x+y)\mathrm{i}\,\middle|\,x,y\in\mathbb{Z}\right\}.$$

令 $1+x-y=a,x+y=b$,解之,得 $x=\dfrac{a+b-1}{2},y=\dfrac{-a+b+1}{2}$. 只有在 a,b 不同奇偶时,x,y 才是整数,从而

$$[1]=\left\{a+bi\,\middle|\,a,b\in\mathbb{Z}\ ,a,b\text{ 不同奇偶}\right\}.$$

又$[0]\cup[1]=R,[0]\cap[1]=\varnothing$,所以 $R/(1+\mathrm{i})=\{[0],[1]\}$.

注　1)　称 $R=\left\{a+bi\,\middle|\,a,b\in\mathbb{Z}\right\}$为高斯(Gauss)数环,记为 $\mathbb{Z}[\mathrm{i}]$.

2)　$\mathbb{Z}[\mathrm{i}]/(1+\mathrm{i})=\{[0],[1]\}$是一个无零因子环,$[1]$是它的单位元. 因 $1[1]=[1]\neq[0]$,而$2[1]=[2]=[(1-\mathrm{i})(1+\mathrm{i})]=(1+\mathrm{i})=[0]$,故$[1]$对于加法来说的阶是 2,从而 $\mathbb{Z}[\mathrm{i}]/(1+\mathrm{i})$的特征是 2.

3)　一般来说,设 m,n 是非负整数,$m^2+n^2\neq 0$,则

$$(m,n)=1\Leftrightarrow\mathbb{Z}\ [\mathrm{i}]/(m+n\mathrm{i})\cong\mathbb{Z}_{m^2+n^2},$$

从而此时 $\mathbb{Z}[\mathrm{i}]/(m+n\mathrm{i})$恰有 m^2+n^2 个元. 例如,$\mathbb{Z}[\mathrm{i}]/(2+\mathrm{i})\cong\mathbb{Z}_5$恰有 $2^2+1^2=5$ 个元.(证明略)

三、讲与练

1. 试判断下面各题中的 S 是否为环 R 的理想.

1) $R=\mathbb{Z}[x], S=\mathbb{Z}$.

2) $R=\mathbb{Z}, S=\mathbb{Z}_3$.

3) R 是交换环,取定 $a\in R$, $S=\{x\in R \mid ax=0\}$.

4) R 是环,取定整数 n, $S=\{a\in R \mid na=0\}$.

5) 取定 $a\in$ 环 K, $S=\{n\in\mathbb{Z} \mid na=0\}$, $R=\mathbb{Z}$.

6) $S=\{n\in\mathbb{Z} \mid na=0, \forall a\in$ 环 $K\}$, $R=\mathbb{Z}$.

7) R 是环,取定整数 n, $S=\{na \mid a\in R\}$.

8) 取定 $a\in$ 环 R, $S=\{ra \mid r\in R\}$.

9) $\mathfrak{A}_1, \mathfrak{A}_2$ 分别是环 R_1, R_2 的理想. $S=\{(a_1,a_2) \mid a_1\in\mathfrak{A}_1, a_2\in\mathfrak{A}_2\}$, $R=\{(r_1,r_2) \mid r_1\in R_1, r_2\in R_2\}$.

10) $R=\mathbb{R}[x]$, $S=\{a_2x^2+a_3x^3+\cdots+a_nx^n \mid a_i\in\mathbb{R}, n$ 是 $\geqslant 2$ 的整数$\}$.

11) $R=F[x]$,其中 F 是数域. 取定 $c\in F$. $S=\{f(x)\in F[x] \mid f(c)=0\}$.

12) $R=M_2(\mathbb{Q})$. $S=\{A \mid A$ 是 $\mathbb{Q}$ 上 2 阶非可逆矩阵$\}$.

13) $R=M_3(\mathbb{Z})$. $S=\left\{\begin{pmatrix}0&a&b\\0&0&c\\0&0&0\end{pmatrix} \middle| a,b,c\in\mathbb{Z}\right\}$.

14) a 是环 R 的中心里的一个固定元, $S=\{x-ax \mid x\in R\}$.

15) $\mathfrak{A}_i$ 是环 R 的理想, $i=1,2,\cdots$, 且 $\mathfrak{A}_1\subset\mathfrak{A}_2\subset\cdots\subset\mathfrak{A}_n\subset\cdots$, $S=\bigcup_{i=1}^{\infty}\mathfrak{A}_i$.

16) K 是环, $\mathfrak{A}$ 是 K 的理想. R 是 K 上的取值在 K 内的全函数环,即 $R=\{f \mid f$ 是 K 的变换$\}$. 环 R 的代数运算为: $(f+g)(x)=f(x)+g(x)$, $(fg)(x)=f(x)g(x)$, $\forall x\in K$ (见第九章,三,9,注 3)). $S=\{f\in R \mid f(\mathfrak{A})\subset\mathfrak{A}\}$.

解 1) 不是. $\exists 2\in\mathbb{Z}$, $x\in\mathbb{Z}[x]$,使得 $2x\,\overline{\in}\,\mathbb{Z}$.

2) 不是. 因 $\mathbb{Z}_3\not\subset\mathbb{Z}$.

3) 是. 事实上,由第十一章,四,4,3)已知 S 是 R 的一个子环. $\forall r\in R, x\in S$,因 R 是交换环,故 $a(rx)=(ax)r=0r=0$,从而 $rx\in S$. 同理 $xr\in S$. 所以 S 是 R 的理想.

4) 是. 事实上,因 $0\in S$,故 $S\neq\varnothing$. 显然 $S\subset R$. $\forall a,b\in S$,有 $na=nb=0$,从而 $n(a-b)=na-nb=0-0=0$,于是 $a-b\in S$. $\forall a\in S, r\in R$, $n(ra)=r(na)=r0=0$,从而 $ra\in S$. 同理 $ar\in S$. 所以 S 是 R 的理想.

5) 是. 事实上,因 $0\in S$,故 $S\neq\varnothing$. 显然 $S\subset R$. $\forall n,m\in S$, $(n-m)a=na-ma=0-0=0$,于是 $n-m\in S$. $\forall r\in R, n\in S$, $(rn)a=r(na)=r0=0$,于是 $ra\in S$. 同理 $ar\in S$. 所以 S 是 R 的理想.

6) 是. 事实上,因 $0\in S$,故 $S\neq\varnothing$. 显然 $S\subset R$. $\forall n,m\in S$, $\forall a\in$ 环 K, $na=0$, $ma=0$,从而 $(n-m)a=na-ma=0-0=0$. 于是 $n-m\in S$. $\forall r\in R$, $\forall n\in S$, $\forall a\in K$, $na=0$,从而 $(rn)a=r(na)=r0=0$,从而 $rn\in S$. 同理 $nr\in S$. 所以 S 是 R 的理想.

7）是. 事实上，因 $0=n0\in S$，故 $S\neq\varnothing$. 显然 $S\subset R$. $\forall\, na, nb\in S$，因 $a-b\in R$，故 $na-nb=n(a-b)\in S$. $\forall\, r\in R, na\in S$，因 $ra\in R$，故 $r(na)=n(ra)\in S$. 同理 $(na)r\in S$. 所以 S 是 R 的理想.

8）不是. 例，设环 $R=\left\{\begin{pmatrix} a & b\\ 0 & 0\end{pmatrix}\middle| a,b\in\mathbb{Z}\right\}$. 取定 $\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\in R$，此时 $S=\left\{\begin{pmatrix} a & b\\ 0 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\middle| a,b\in\mathbb{Z}\right\}=\left\{\begin{pmatrix} a & 0\\ 0 & 0\end{pmatrix}\middle| a\in\mathbb{Z}\right\}$. 取 $\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\in S$，$\begin{pmatrix}2 & 3\\ 0 & 0\end{pmatrix}\in R$，但 $\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}2 & 3\\ 0 & 0\end{pmatrix}=\begin{pmatrix}2 & 3\\ 0 & 0\end{pmatrix}\overline{\in} S$. 所以 S 不是 R 的理想. 由第十二章，二，6，注 4）知 $S=\{ra\mid r\in R\}$ 是 R 的左理想.

9）是. 事实上，由第十章，三，2，注 1）知 S 是 R 的子环. $\forall\,(r_1,r_2)\in R, (a_1,a_2)\in S$，其中 $r_i\in R_i, a_i\in\mathfrak{A}_i$，因 $\mathfrak{A}_i$ 是 R_i 的理想. 故 $r_ia_i, a_ir_i\in\mathfrak{A}_i, i=1,2$，从而 $(r_1,r_2)(a_1,a_2)=(r_1a_1, r_2a_2)\in S$，$(a_1,a_2)(r_1,r_2)=(a_1r_1,a_2r_2)\in S$. 所以 S 是 R 的理想.

10）是. 事实上，因 $0\in S$，故 $S\neq\varnothing$. 显然 $S\subset R$. $\forall\ \sum\limits_{i=2}^{n}a_ix^i, \sum\limits_{i=2}^{m}b_ix^i\in S$，不妨设 $n\geqslant m$，则 $\sum\limits_{i=2}^{n}a_ix^i-\sum\limits_{i=2}^{m}b_ix^i=\sum\limits_{i=2}^{n}(a_i-b_i)x^i\in S$，其中 $b_{m+1}=\cdots=b_n=0$. $\forall\ \sum\limits_{i=0}^{t}r_ix^i\in R$，$\forall\ \sum\limits_{j=2}^{n}a_jx^j\in S$，$\left(\sum\limits_{i=0}^{t}r_ix^i\right)\left(\sum\limits_{j=2}^{n}a_jx^j\right)=\sum\limits_{k=2}^{t+n}\left(\sum\limits_{i+j=k}^{t+n}r_ia_j\right)x^k\in S$. 同理 $\left(\sum\limits_{j=2}^{n}a_jx^j\right)\left(\sum\limits_{i=0}^{t}r_ix^i\right)\in S$. 所以 S 是 R 的理想.

注　类似地，$\left\{a_3x^3+\cdots+a_nx^n\,\middle|\, a_i\in\mathbb{R}[x], n\text{ 是}\geqslant 3\text{ 的整数}\right\}$，$\left\{a_4x^4+\cdots+a_nx^n\,\middle|\, a_i\in\mathbb{R}, n\text{ 是}\geqslant 4\text{ 的整数}\right\}$，…都是 $\mathbb{R}[x]$ 的理想.

11）是. 事实上，因 $0\in S$，故 $S\neq\varnothing$. 显然 $S\subset R$. $\forall\, f(x), g(x)\in S$，有 $f(c)=g(c)=0$. 令 $h(x)=f(x)-g(x)$，于是 $h(c)=f(c)-g(c)=0-0=0$，从而 $h(x)=f(x)-g(x)\in S$. $\forall\, r(x)\in R$，$\forall\, f(x)\in S$，有 $f(c)=0$. 令 $k(x)=r(x)f(x)$，于是 $k(c)=r(c)f(c)=r(c)0=0$，从而 $k(x)=r(x)f(x)\in S$. 同理 $f(x)r(x)\in S$. 所以 S 是 R 的理想.

注　S 是由 $x-c$ 生成的主理想，即 $S=(x-c)$. 事实上，$\forall\, f(x)\in S$，有 $f(c)=0$，即 $x-c\mid f(x)$，从而 $\exists\, q(x)\in R$，使得 $f(x)=q(x)(x-c)\in(x-c)$. 于是 $S\subset(x-c)$. 反之，$\forall\, g(x)\in(x-c)$，因 R 是有单位元的交换环，故 $\exists\, u(x)\in R$，使得 $g(x)=u(x)(x-c)$，从而 $x-c\mid g(x)$，即 $g(c)=0$. 因此 $g(x)\in S$. 于是 $(x-c)\subset S$. 所以 $S=(x-c)$.

12）不是. 取 $\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 0 & -1\end{pmatrix}\in S$，但 $\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}-\begin{pmatrix}0 & 0\\ 0 & -1\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\overline{\in} S$，从而 S 不是 R 的理想.

13）不是. 取 $\begin{pmatrix}1 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 1\end{pmatrix}\in R$，$\begin{pmatrix}0 & a & b\\ 0 & 0 & c\\ 0 & 0 & 0\end{pmatrix}\in S$ 而其中 $a\neq 0$，于是

$$\begin{pmatrix}1 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 1\end{pmatrix}\begin{pmatrix}0 & a & b\\ 0 & 0 & c\\ 0 & 0 & 0\end{pmatrix}=\begin{pmatrix}0 & a & b+c\\ 0 & a & b+c\\ 0 & a & b+c\end{pmatrix}\overline{\in} S.$$

从而 S 不是 R 的理想.

14) 是. 因 $0=0-a0\in S$, 故 $S\neq\varnothing$. 显然 $S\subset R$. $\forall x-ax, y-ay\in S$, $(x-ax)-(y-ay)=(x-y)-a(x-y)\in S$. $\forall r\in R$, $\forall x-ax\in S$, 因 a 在 R 的中心里, 故 $ra=ar$, 从而 $r(x-ax)=rx-rax=rx-a(rx)\in S$. 同理 $(x-ax)r\in S$. 所以 S 是 R 的理想.

15) 是. 事实上, 因 $0\in S$, 故 $S\neq\varnothing$. 显然 $S\subset R$. $\forall a,b\in S$, 不妨设 $a\in\mathfrak{A}_n$, $b\in\mathfrak{A}_m$, $n\leqslant m$, 则 $a\in\mathfrak{A}_m$. 因 $\mathfrak{A}_m$ 是理想, 故 $a-b\in\mathfrak{A}_m\subset S$. $\forall r\in R$, $a\in S$, 不妨设 $a\in\mathfrak{A}_n$. 因 $\mathfrak{A}_n$ 是理想, 故 $ra\in\mathfrak{A}_n\subset S$, $ar\in\mathfrak{A}_n\subset S$. 所以 S 是 R 的理想.

16) 是. 事实上, 零变换 0(即把 K 中任意元都映到 K 中的零元的变换)$\in R$, 且 $0(\mathfrak{A})=\{0\}\subset\mathfrak{A}$, 从而 $0\in S$, 于是 $S\neq\varnothing$. 显然 $S\subset R$. $\forall f,g\in S$, 有 $f(\mathfrak{A})\subset\mathfrak{A}$, $g(\mathfrak{A})\subset\mathfrak{A}$, $f-g\in R$. $\forall a\in\mathfrak{A}$, 由 $f(a)\in\mathfrak{A}$, $g(a)\in\mathfrak{A}$, $\mathfrak{A}$ 是理想, 有 $(f-g)(a)=f(a)-g(a)\in\mathfrak{A}$, 于是 $(f-g)(\mathfrak{A})\subset\mathfrak{A}$. 因此 $f-g\in S$. $\forall h\in R$, $f\in S$, 有 $f(\mathfrak{A})\subset\mathfrak{A}$, $hf\in R$. $\forall a\in\mathfrak{A}$, 因 $\mathfrak{A}$ 是 K 的理想, 故 $(hf)(a)=h(a)f(a)\in K\mathfrak{A}\subset\mathfrak{A}$. 于是 $(hf)(\mathfrak{A})\subset\mathfrak{A}$. 因此 $hf\in S$. 同理 $fh\in S$. 所以 S 是 R 的理想.

2. 证明:整数环 $\mathbb{Z}$ 的每一理想 $\mathfrak{A}$ 都是 $\mathbb{Z}$ 的主理想.

证一 若 $\mathfrak{A}=\{0\}$, 则 $\mathfrak{A}$ 是主理想 (0).

若 $\mathfrak{A}\neq\{0\}$, 则 $\exists a(\neq 0)\in\mathfrak{A}$. 因 $\mathfrak{A}$ 是加群, 故 $-a\in\mathfrak{A}$, a 与 $-a$ 二者中必有一个是正整数, 从而 $\mathfrak{A}$ 中有正整数. 于是集 $A=\left\{x\in\mathfrak{A}\,\middle|\,x \text{ 是正整数}\right\}\neq\varnothing$. 所以 A 中有最小正整数 a, 我们有 $\mathfrak{A}=(a)$. 事实上, $\forall b\in\mathfrak{A}$, $\exists q,r\in\mathbb{Z}$, 使得 $b=qa+r$, $0\leqslant r<a$. 由 $\mathfrak{A}$ 是理想, $r=b-qa\in\mathfrak{A}$. 由 a 是 A 中最小正整数, 又 $0\leqslant r<a$, 因此 $r=0$, 从而 $b=qa\in(a)$, 即 $\mathfrak{A}\subset(a)$. 反之, 由 $a\in\mathfrak{A}$, $\mathfrak{A}$ 是理想, $(a)\subset\mathfrak{A}$. 所以 $\mathfrak{A}=(a)$.

证二 因整数环 $\mathbb{Z}$ 是循环加群, 故 $\mathbb{Z}$ 的任一理想 $\mathfrak{A}$ 是加群 $\mathbb{Z}$ 的由 $\mathbb{Z}$ 的某个元 a 生成的循环子加群, 即 $\mathfrak{A}=\left\{ma\,\middle|\,m\in\mathbb{Z}\right\}$. 因 $\mathbb{Z}$ 是有单位元的交换环, 故 $\mathfrak{A}$ 就是由 a 生成的主理想, 即 $\mathfrak{A}=\left\{ma\,\middle|\,m\in\mathbb{Z}\right\}=(a)$.

注 1) 因为对于任意整数 a 来说, 有 $(a)=(-a)$, 所以 $\mathbb{Z}$ 的任一理想都是由一个非负整数生成的主理想.

2) 整数加群 $\mathbb{Z}$ 的任意一个子加群都是整数环 $\mathbb{Z}$ 的理想, 从而整数环 $\mathbb{Z}$ 的每一个子环都是 $\mathbb{Z}$ 的理想.

3) 整数环 $\mathbb{Z}$ 的理想有无穷多个. 事实上, $\forall$ 正整数 n, 因 $\mathbb{Z}$ 是有单位元的交换环, 故 $(n)=\left\{rn\,\middle|\,r\in\mathbb{Z}\right\}$ 是 $\mathbb{Z}$ 的理想. 当 m,n 是两个不同的正整数时, 不妨设 $n>m$, 则 $m\notin(n)$. 否则, 若 $m\in(n)$, 则 $\exists q\in\mathbb{Z}$, 使得 $qn=m$. 如果 $q>0$, 那么 $qn>n>m$, 矛盾. 如果 $q\leqslant 0$, 那么 $qn\leqslant 0<m$, 矛盾. 所以 $m\notin(n)$, 即 $(m)\neq(n)$. 因正整数有无穷多个, 故 $\mathbb{Z}$ 的理想有无穷多个.

4) 整数环 $\mathbb{Z}$ 的全部剩余类环恰是 $\mathbb{Z}/(m)=\mathbb{Z}_m$, 其中 m 取遍所有的非负整数, 特别地, 当 $m=0$ 时, $\mathbb{Z}/(m)=\mathbb{Z}/(0)\cong\mathbb{Z}$.

5) 设 $a,b\in\mathbb{Z}$, 则

$$(a,b)=(d)\Leftrightarrow d \text{ 是 } a,b \text{ 的最大公因子}.$$

事实上, 由第十二章, 二, 4, 注 5), $(a,b)=(a)+(b)$. 由第十二章, 二, 4, 注 4),

$$(a)+(b)=(d)\Leftrightarrow d \text{ 是 } a,b \text{ 的最大公因子},$$

所以结论成立.

例 因 2 是 4 与 10 的最大公因子, 故 $(4,10)=(2)$. 又 $(10,13)=(1)=\mathbb{Z}$.

6）　该命题的证法有一般性，仿此可证明：数域 F 上的一元多项式环 $F[x]$ 的任意理想都是主理想.

事实上，设$\mathfrak{A}$是 $F[x]$ 的一个理想. 若$\mathfrak{A}=\{0\}$，则$\mathfrak{A}$是主理想(0). 若$\mathfrak{A}\neq\{0\}$，则 $\exists f(x)\in\mathfrak{A}$，$f(x)\neq 0$，从而集 $A=\left\{\deg h(x)\,\middle|\,h(x)\in\mathfrak{A},h(x)\neq 0\right\}\neq\varnothing$. 于是 $\exists$ 次数最小的多项式 $g(x)\in\mathfrak{A}$，则$\mathfrak{A}=(g(x))$. 这是因为 $\forall k(x)\in\mathfrak{A}$，因在数域 F 上的多项式环 $F[x]$ 中，带余除法定理成立，故 $\exists q(x),r(x)\in F[x]$，使得 $k(x)=q(x)g(x)+r(x)$，其中 $r(x)=0$ 或 $\deg r(x)<\deg g(x)$. 根据$\mathfrak{A}$是理想，$r(x)=k(x)-q(x)g(x)\in\mathfrak{A}$. 若 $r(x)\neq 0$，则 $\deg r(x)<\deg g(x)$. 此与 $g(x)$ 是$\mathfrak{A}$中次数最小的多项式这一假设矛盾，从而 $r(x)=0$. 即 $k(x)=q(x)g(x)\in(g(x))$. 于是$\mathfrak{A}\subset(g(x))$. 反之，因 $g(x)\in\mathfrak{A}$，$\mathfrak{A}$是理想，故$(g(x))\subset\mathfrak{A}$. 所以$\mathfrak{A}=(g(x))$.

该命题可推广为：任意域 F 上的一元多项式环 $F[x]$ 的每个理想都是主理想.

7）　$\mathbb{Z}_n$的任一理想都是主理想，且$\mathbb{Z}_n$的理想的个数等于 n 的正因子的个数. 证明见第十二章，二，5，注 1)，2).

3. 举例说明，环 R 的理想$\mathfrak{A}$的理想$\mathfrak{A}_1$ 未必是 R 的理想. 即理想不具有传递性.

解　例，设环 $R=\left\{a+b\mathrm{i}\,\middle|\,a,b\in\mathbb{Z}\right\}$，$\mathfrak{A}=\left\{4a+4b\mathrm{i}\,\middle|\,a,b\in\mathbb{Z}\right\}$，$\mathfrak{A}_1=\left\{8a+4b\mathrm{i}\,\middle|\,a,b\in\mathbb{Z}\right\}$，则容易验证：$\mathfrak{A}_1$ 是$\mathfrak{A}$的理想，$\mathfrak{A}$是 R 的理想. 但$\mathfrak{A}_1$ 不是 R 的理想. 比如，取 $1+\mathrm{i}\in R$，$8+4\mathrm{i}\in\mathfrak{A}_1$，而$(1+\mathrm{i})(8+4\mathrm{i})=4+12\mathrm{i}\,\overline{\in}\,\mathfrak{A}_1$.

又例　设

$$R=\left\{\begin{pmatrix}0&a&b\\0&c&d\\0&0&e\end{pmatrix}\,\middle|\,a,b,c,d,e\in\mathbb{Z}\right\},$$

$$\mathfrak{A}=\left\{\begin{pmatrix}0&0&b\\0&0&d\\0&0&0\end{pmatrix}\,\middle|\,b,d\in\mathbb{Z}\right\},\quad \mathfrak{A}_1=\left\{\begin{pmatrix}0&0&0\\0&0&d\\0&0&0\end{pmatrix}\,\middle|\,d\in\mathbb{Z}\right\}.$$

易验证$\mathfrak{A}_1$ 是$\mathfrak{A}$的理想，$\mathfrak{A}$是环 R 的理想. 但$\mathfrak{A}_1$ 不是 R 的理想，比如取

$$\begin{pmatrix}0&1&0\\0&0&0\\0&0&0\end{pmatrix}\in R,\quad \begin{pmatrix}0&0&0\\0&0&2\\0&0&0\end{pmatrix}\in\mathfrak{A}_1,$$

而

$$\begin{pmatrix}0&1&0\\0&0&0\\0&0&0\end{pmatrix}\begin{pmatrix}0&0&0\\0&0&2\\0&0&0\end{pmatrix}=\begin{pmatrix}0&0&2\\0&0&0\\0&0&0\end{pmatrix}\overline{\in}\,\mathfrak{A}_1.$$

注　1）　环 R 的左理想 S_1 的左理想 S_2 未必是 R 的左理想. 例，设 S 是环. $S_1=\left\{\begin{pmatrix}a&0\\b&0\end{pmatrix}\,\middle|\,a,b\in S\right\}$，$S_2=\left\{\begin{pmatrix}0&0\\c&0\end{pmatrix}\,\middle|\,c\in S\right\}$. 显然 S_1 是 $M_2(S)$ 的子环，S_2 是 S_1 的子环. $\forall\begin{pmatrix}x&y\\u&v\end{pmatrix}\in M_2(S)$，$\begin{pmatrix}a&0\\b&0\end{pmatrix}\in S_1$，$\begin{pmatrix}0&0\\c&0\end{pmatrix}\in S_2$，由 $\begin{pmatrix}x&y\\u&v\end{pmatrix}\begin{pmatrix}a&0\\b&0\end{pmatrix}=\begin{pmatrix}ax+by&0\\au+bv&0\end{pmatrix}\in S_1$，知 S_1 是 $M_2(S)$ 的左理想. 由 $\begin{pmatrix}a&0\\b&0\end{pmatrix}\begin{pmatrix}0&0\\c&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}\in S_2$，知 S_2 是 S_1 的左理想，但取

$\begin{pmatrix}0&1\\0&0\end{pmatrix}\in M_2(S)$，$\begin{pmatrix}0&0\\1&0\end{pmatrix}\in S_2$，而$\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&0\\1&0\end{pmatrix}=\begin{pmatrix}1&0\\0&0\end{pmatrix}\overline{\in} S_2$. 所以 S_2 不是 $M_2(S)$的左理想.

2）设$\mathfrak{A}$是环 R 的理想，$\mathfrak{A}$有单位元 1，$\mathfrak{A}_1$ 是$\mathfrak{A}$的理想，则$\mathfrak{A}_1$ 是 R 的理想. 事实上，显然$\mathfrak{A}_1$ 是R的子环. 因1是$\mathfrak{A}$的单位元，故$\forall r\in R, a\in\mathfrak{A}_1\subset\mathfrak{A}$，有$1a=a1=a$，从而$ra=r(1a)=(r1)a$. 因$\mathfrak{A}$是 R 的理想，故 $r1\in R\,\mathfrak{A}\subset\mathfrak{A}$. 又因$\mathfrak{A}_1$是$\mathfrak{A}$的理想，故 $ra=(r1)a\in\mathfrak{A}\mathfrak{A}_1\subset\mathfrak{A}_1$. 同理 $ar=(a1)r=a(1r)\in\mathfrak{A}_1(\mathfrak{A}\,R)\subset\mathfrak{A}_1\,\mathfrak{A}\subset\mathfrak{A}_1$. 所以$\mathfrak{A}_1$ 是 R 的理想.

3）首先给出定义：设$\mathfrak{A}$是交换环，$\mathfrak{A}_1$ 是$\mathfrak{A}$的理想. 若$\forall a,b\in\mathfrak{A}, ab\in\mathfrak{A}_1$，有 $a\in\mathfrak{A}_1$ 或 $b\in\mathfrak{A}_1$，则称$\mathfrak{A}_1$ 是$\mathfrak{A}$的素理想. 我们有下面结论：交换环 R 的理想$\mathfrak{A}$的素理想$\mathfrak{A}_1$ 是 R 的理想. 事实上，若$\mathfrak{A}_1=\mathfrak{A}$，显然$\mathfrak{A}_1$是$R$的理想. 若$\mathfrak{A}_1\neq\mathfrak{A}$，但$\mathfrak{A}_1\subset\mathfrak{A}$，则$\exists\, a\in\mathfrak{A}, a\overline{\in}\mathfrak{A}_1$. $\forall\, b\in\mathfrak{A}_1$，$\forall\, r\in R$，因$\mathfrak{A}$是 R 的理想，故 $ra\in\mathfrak{A}$. 因$\mathfrak{A}_1$ 是$\mathfrak{A}$的理想，故$(ra)b\in\mathfrak{A}_1$. 又 R 是交换环，于是$a(rb)=(ra)b\in\mathfrak{A}_1$. 但 $a\overline{\in}\mathfrak{A}_1$，$\mathfrak{A}_1$ 是 a 的素理想，因此 $rb\in\mathfrak{A}_1$. 由$\mathfrak{A}_1$ 是交换环，$br\in\mathfrak{A}_1$，又$\mathfrak{A}_1$ 是加群，所以$\mathfrak{A}_1$ 是 R 的理想.

4. 在整数环 $\mathbb{Z}$ 的模理想(19)的剩余类环 $\mathbb{Z}/(19)$中，模(19)的剩余类[6]在 $\mathbb{Z}/(19)$中是否有逆元？若有，试求之.

解 $\mathbb{Z}/(19)=\mathbb{Z}_{19}$，而 19 是素数，因此 $\mathbb{Z}/(19)$是域，所以$[6](\neq[0])$在 $\mathbb{Z}/(19)$中有逆元. 设$[a]$是$[6]$的逆元，则$[6][a]=[6a]=[1]$，从而 $19\mid 6a-1$. 取 $a=-3$ 即可. 于是$[6]^{-1}=[-3]=[16]$.

5. 设 $2\mathbb{Z}$ 是偶数环，问环 $2\mathbb{Z}/(4)$含多少元？

解 因 $2\mathbb{Z}$ 是交换环，故

$$
\begin{aligned}
(4)&=\left\{4r+n4 \,\middle|\, r\in 2\mathbb{Z}, n\in\mathbb{Z}\right\}=\left\{(r+n)4 \,\middle|\, r\in 2\mathbb{Z}, n\in\mathbb{Z}\right\}\\
&=\left\{4k \,\middle|\, k\in\mathbb{Z}\right\}.
\end{aligned}
$$

$\forall\, 2n_1, 2n_2\in 2\mathbb{Z}, n_1, n_2\in\mathbb{Z}$，

$$
\begin{aligned}
2n_1, 2n_2 \text{ 属于同一个模(4)的剩余类} &\Leftrightarrow 2n_1-2n_2\in(4)\\
&\Leftrightarrow 2n_1-2n_2=4k, k\in\mathbb{Z}\\
&\Leftrightarrow n_1-n_2=2k, k\in\mathbb{Z}\\
&\Leftrightarrow n_1, n_2 \text{ 同奇偶}.
\end{aligned}
$$

因此 $2\mathbb{Z}/(4)$有且只有以下两个元：

$$
\begin{aligned}
\left\{2n \,\middle|\, n\text{ 是偶数}\right\}&=\left\{2\cdot 2k \,\middle|\, k\in\mathbb{Z}\right\}=(4)=[0],\\
\left\{2n \,\middle|\, n\text{ 是奇数}\right\}&=\left\{2(2k+1) \,\middle|\, k\in\mathbb{Z}\right\}\\
&=\left\{2+4k \,\middle|\, k\in\mathbb{Z}\right\}=2+(4)=[2].
\end{aligned}
$$

所以 $2\mathbb{Z}/(4)=\{[0],[2]\}$.

6. 设 R 是有单位元的交换环.

1）证明：$\forall f(x)\in R[x]$，$\phi: f(x)\to f(0)$（这里 0 是 R 的零元）是$R[x]$到 R 的一个同态满射.

2）求出ϕ的核 $\ker\phi$.

3）$R[x]/\ker\phi$与哪个环同构？

证　1)　$\forall f(x)\in R[x]$，$\exists | f(0)\in R$，使得$\phi(f(x))=f(0)$，所以ϕ是映射. $\forall a\in R$，$\exists f(x)=a\in R[x]$，使得$\phi(f(x))=\phi(a)=f(0)=a$，所以$\phi$是满射. $\forall f(x),g(x)\in R[x]$，

$$\phi(f(x)+g(x))=f(0)+g(0)=\phi(f(x))+\phi(g(x)),$$

$$\phi(f(x)g(x))=f(0)g(0)=\phi(f(x))\phi(g(x)).$$

所以ϕ保持运算，从而ϕ是 $R[x]$到 R 的一个同态满射.（还可如下证明：因 R 是有单位元的交换环，故 $R[x]$是 R 上未定元多项式环. 于是 $R[x]\overset{\phi}{\sim}R[0]$，且$\phi$: $f(x)\to f(0)$. 又多项式环 $R[0]=R$，从而ϕ: $f(x)\to f(0)$是 $R[x]$到 R 的一个同态满射.）

2)　$\ker\phi=\{f(x)\in R[x]\,|\,\phi(f(x))=f(0)=0\}$

$=\{f(x)\in R[x]\,|\,f(x)\text{不含零次项}\}$

$=\{a_1x+a_2x^2+\cdots+a_nx^n\,|\,a_i\in R,n\text{ 是正整数}\}$

$=\{xf(x)\,|\,f(x)\in R[x]\}=(x)$.

3)　由同态基本定理，$R[x]/(x)\cong R$.（还可如下证明：因 $R[x]/(x)=\{[f(x)]\,|\,f(x)\in R[x]\}$，又

a 是 $f(x)$的常数项 $\Leftrightarrow x\,|\,f(x)-a$

$$\Leftrightarrow f(x)-a=xq(x)\in(x)\Leftrightarrow[f(x)]=[a].$$

故 $R[x]/(x)=\{[a]\,|\,a\in R\}$. 于是 ψ:$[a]\to a$ 是 $R[x]/(x)$与 R 间的一个同构映射. 事实上，$\forall[a]\in R[x]/(x)$，$\exists a\in R$，使得 $\psi([a])=a$. 若$[b]=[a]$，则 $b-a\in(x)$，从而 $\exists q(x)\in R[x]$，使得 $b-a=xg(x)$，即 $x\,|\,b-a$，因此 $b=a$. 所以 ψ 是映射. 显然 ψ 是满射且保持运算. 于是 $R[x]/(x)\overset{\psi}{\cong}R$.）

注　与该命题类似地可证明：设 R 是有单位元的交换环. 取定 $b\in R$. 则ϕ:$f(x)\to f(b)$是 $R[x]$到 R 的一个同态满射. 且

$$\ker\phi=\{f(x)\in R[x]\,|\,\phi(f(x))=f(b)=0\}=\{f(x)\in R[x]\,|\,x-b\,|\,f(x)\}$$

$$=\{q(x)(x-b)\,|\,q(x)\in R[x]\}=(x-b),$$

$R[x]/(x-b)\cong R$.

四、思考问题

1. 在实数域$\mathbb{R}$上 x,y 的多项式环$\mathbb{R}[x,y]$中，下面集合 S 哪些是$\mathbb{R}[x,y]$的理想？

1)　$S=\{f(x,y)\in\mathbb{R}[x,y]\,|\,f(x,y)\text{的常数项等于 }0\}$.

2)　$S=\{f(y)\,|\,f(y)\in\mathbb{R}[y]\}$.

3)　$S=\{f(x,y)\in\mathbb{R}[x,y]\,|\,f(x,y)\text{的常数项和一次项系数都为 }0\}$.

4)　$S=\{f(x,y)\in\mathbb{R}[x,y]\,|\,f(x,y)\text{的二次项系数等于 }0\}$.

2. 设 R 是有单位元的交换环，$\mathfrak{A}$是 R 的理想，$S=\{x\in R\,|\,\exists\text{ 正整数 }n\text{，使得 }x^n\in\mathfrak{A}\}$.
证明：

1） S 是 R 的理想.

2） $S \supset \mathfrak{A}$.

3） $S_1 = \left\{ x \in R \,\middle|\, \exists \text{正整数 } n, \text{使得 } x^n \in S \right\} \supset S$.

4） $S = R \Leftrightarrow \mathfrak{A} = R$.

3. 设 R 是有单位元 1 的环，取定 $a_1, a_2, \cdots, a_n \in R$. 证明：

$$S = \left\{ x_1 a_1 + x_2 a_2 + \cdots + x_n a_n \,\middle|\, x_i \in R \right\}$$

是 R 的左理想，且 S 是含 $a_1, a_2 \cdots, a_n$ 的 R 的最小左理想. 称 S 为 R 的由 $a_1, a_2, \cdots, a_n$ 生成的左理想.

4. 若 R 是环，取定 $a \in R$，证明：$S = \left\{ x \in R \,\middle|\, ax = 0 \right\}$ 是 R 的右理想.

5. 设 S 是环 R 的左理想，证明：$\mathfrak{A} = \left\{ x \in R \,\middle|\, xR \subset S \right\}$ 是 R 的理想.

6. 设 R 是交换环，证明：

1） $\mathfrak{A} = \left\{ a \,\middle|\, a \text{ 是 } R \text{ 的幂零元} \right\}$ 是 R 的理想.

2） $R/\mathfrak{A}$ 中只有零元[0]是幂零元.

7. 证明：

1） 设 S 是环 R 的右理想，则 $\mathfrak{A} = \left\{ x \in R \,\middle|\, Sx = \{0\} \right\}$ 是 R 的理想，称 $\mathfrak{A}$ 为 S 在 R 中的右零化子.

2） 设 S 是环 R 的左理想，则 $\mathfrak{B} = \left\{ y \in R \,\middle|\, yS = \{0\} \right\}$ 是 R 的理想，称 $\mathfrak{B}$ 为 S 在 R 中的左零化子.

8. 设环 R 除本身和 $\{0\}$ 外，没有其他的左理想. 证明：R 是除环或幂零元环（见第九章，四，12，6））.

9. 设 Z 是环 R 的中心，$e \in Z$，称 e 为 R 的中心元. 又设 R 有单位元 1，证明：

1） 若 e 是 R 的中心元，则 $1-e$ 也是.

2） 若 e 是 R 的幂等元，则 $1-e$ 也是.

3） 若 e 是 R 的中心元，则 eR 和 $(1-e)R$ 都是 R 的理想.

10. 设 R 是非零整环，且只含有限个理想，证明：R 是除环.

11. $\mathfrak{A} = ([2]x + [3])$ 是环 $\mathbb{Z}_5[x]$ 的理想. 在 $\mathbb{Z}_5[x]$ 的模 $\mathfrak{A}$ 的剩余类环 $\mathbb{Z}_5[x]/\mathfrak{A}$ 中，求出 $([3]x^2 - [1]x + [1]) + \mathfrak{A}$ 与 $([2]x - [1]) + \mathfrak{A}$ 的积.

12. 设 F 是域，证明：$F[x]/(x^2 - 1)$ 有零因子.

13. 证明下面各题中的 ϕ 是环 R 到环 $\overline{R}$ 的一个同态满射. 求出 $\ker \phi$ · $R/\ker \phi$ 与哪个环同构.

1） $R = \mathbb{Z}[x]$，$\overline{R} = \mathbb{Z}[\mathrm{i}] = \left\{ a + b\mathrm{i} \,\middle|\, a, b \in \mathbb{Z} \right\}$ 是高斯数环. $\phi: f(x) \to f(\mathrm{i})$.

2） $R = \mathbb{R}[x]$，$\overline{R} = \mathbb{C}$ 是复数域. $\phi: f(x) \to f(\mathrm{i})$.

3） $R = \left\{ (a, b) \,\middle|\, a, b \in \mathbb{Z} \right\}$，$\overline{R} = \mathbb{Z}$. $\phi: (a, b) \to a$[①].

4） $R = \mathbb{Z}$，$\overline{R} = \{[0], [3]\}$，其中[0]，[3]是模 6 的剩余类. ϕ：当 a 是偶数时，$a \to [0]$；

---

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 98. 例 4.

当 a 是奇数时，$a\to[3]$.

5）$R=\mathbb{Z}$，$\overline{R}=\{[0],[2],[4]\}$，其中$[0],[2],[4]$是模 6 的剩余类.

$$\begin{aligned}\phi:\ a&\to[0],\ 4a=6q+0,\\ a&\to[2],\ 4a=6q+2,\\ a&\to[4],\ 4a=6q+4,\end{aligned}$$

其中 $q\in\mathbb{Z}$.

6）m,r 是两个正整数且 $r\mid m$. $R=\mathbb{Z}_m$，$\overline{R}=\mathbb{Z}_r$. 用 $\overline{a}(\in\mathbb{Z}_m)$表示 a 所在的模 m 的剩余类，$[a](\in\mathbb{Z}_r)$表示 a 所在的模 r 的剩余类. $\phi:\overline{a}\to[a]$.

7）$R=\left\{\begin{pmatrix}a&b\\0&c\end{pmatrix}\middle|\,a,b,c\in\mathbb{Z}\right\}$，$\overline{R}=\left\{\begin{pmatrix}a&0\\0&c\end{pmatrix}\middle|\,a,c\in\mathbb{Z}\right\}$. $\phi:\begin{pmatrix}a&b\\0&c\end{pmatrix}\to\begin{pmatrix}a&0\\0&c\end{pmatrix}$.

8）$R=\left\{\begin{pmatrix}a&b\\0&c\end{pmatrix}\middle|\,a,b,c\in\mathbb{Z}\right\}$，$\overline{R}=\left\{\begin{pmatrix}0&0\\0&c\end{pmatrix}\middle|\,c\in\mathbb{Z}\right\}$. $\phi:\begin{pmatrix}a&b\\0&c\end{pmatrix}\to\begin{pmatrix}0&0\\0&c\end{pmatrix}$.

9）$R=M_2(\mathbb{Z})$，$\overline{R}=\left\{\begin{pmatrix}[a]&[b]\\ [c]&[d]\end{pmatrix}\middle|\,[a],[b],[c],[d]\in\mathbb{Z}_2\right\}$.

$$\phi:\begin{pmatrix}a&b\\c&d\end{pmatrix}\to\begin{pmatrix}[a]&[b]\\ [c]&[d]\end{pmatrix}.$$

10）环 $S\overset{\psi}{\sim}$环 $\overline{S}$，$\ker\psi=\mathfrak{A}$. $R=M_n(S)$，$\overline{R}=M_n(\overline{S})$. $\phi:(a_{ij})_n\to(\psi(a_{ij}))_n$.

11）环 $S\overset{\psi}{\sim}$环 $\overline{S}$，$\ker\psi=\mathfrak{A}$. $R=S[x]$，$\overline{R}=\overline{S}[x]$.

$$\phi:f(x)=a_0+a_1x+\cdots+a_nx^n\to\psi(a_0)+\psi(a_1)x+\cdots+\psi(a_n)x^n.$$

14. 设 p 是素数，证明：$\mathbb{Z}/(p^n)$的任一非零理想包含元$[p^{n-1}]$. 即 $\mathbb{Z}/(p^n)$的所有非零理想的交不等于$\{[0]\}$.

15. 设$\mathfrak{A}$是环 R 的理想，且$\mathfrak{A}$，$R/\mathfrak{A}$都是幂零元环（第九章，四，12,6)）. 证明：R 也是幂零元环.

16. 设$\mathfrak{A}$，$\mathfrak{B}$是环 R 的两个理想，且$\mathfrak{A}$，$\mathfrak{B}$都是幂零元环. 证明：$\mathfrak{A}+\mathfrak{B}$也是 R 的理想且是幂零元环.

17. 设$\mathbb{Z}\overset{\phi}{\sim}R$，证明：环 R 的任一子环 S 都是 R 的理想.

第十三章　最大理想、商域

一、基本问题问答

1. 回答下列各问题.

1)　最大理想(也称极大理想)的定义是什么?

2)　环 R 的最大理想是 R 的除单位理想 R 外的所有理想中的最大的一个吗?

3)　环 R 的单位理想 R 和零理想 $\{0\}$ 是 R 的最大理想吗?

4)　环 R 的最大理想一定存在吗?

5)　环 R 的最大理想是唯一的吗?

答　1)　$\mathfrak{A}$是环 R 的最大理想 $\Leftrightarrow$ ①　$\mathfrak{A}$是环 R 的理想;

②　$\mathfrak{A}\neq R$;

③　除$\mathfrak{A}$,R 外,R 没有包含$\mathfrak{A}$的理想

$\Leftrightarrow$ ①　$\mathfrak{A}$是环 R 的理想;

②　$\mathfrak{A}\neq R$;

③　若$\mathfrak{B}$是 R 的理想,$\mathfrak{B}\supset\mathfrak{A}$,$\mathfrak{B}\neq\mathfrak{A}$,则$\mathfrak{B}=R$.

$\Leftrightarrow$ ①　$\mathfrak{A}$是环 R 的理想;

②　$\mathfrak{A}\neq R$;

③　在$\mathfrak{A}$与 R 间,不存在中间理想,即 $\overline{\exists}$ 理想$\mathfrak{B}$,使得 $\mathfrak{A}\subsetneqq\mathfrak{B}\subsetneqq R$.

2)　不是.例,(2)是整数环 $\mathbb{Z}$ 的最大理想,(3)($\neq\mathbb{Z}$)是 $\mathbb{Z}$ 的一个理想,但因 $3\ \overline{\in}(2)$,故 $(2)\not\supset(3)$.

3)　环 R 的单位理想 R 一定不是 R 的最大理想.环 R 的零理想 $\{0\}$ 有可能是 R 的最大理想.对于有且只有零理想和单位理想的环 R 来说(如除环、域),单位理想不是 R 的最大理想.由定义知,零理想 $\{0\}$ 是 R 的最大理想.即

环 R 有且只有零理想和单位理想 $\Leftrightarrow$ 环 R 有且只有零理想是最大理想.

4)　不一定.如零环 $\{0\}$ 没有最大理想.又例,设 $\mathbb{Q}$ 是有理数加群.规定 $\forall a,b\in R,ab=0$. $\mathbb{Q}$ 作成一个环.则 $\mathbb{Q}$ 没有最大理想.

为证此事实,首先证明一个命题:设 $\mathbb{Q}$ 是有理数加群,H 是 $\mathbb{Q}$ 的任一子加群,$H\neq\mathbb{Q}$,$H\neq\{0\}$,则 $\exists$ $\mathbb{Q}$ 的子加群 $\overline{H}$,$\overline{H}\neq\mathbb{Q}$,$\overline{H}\neq H$,但 $\overline{H}\supset H$.

因 $H<\mathbb{Q}$,$H\neq\mathbb{Q}$,故 $\exists a\in\mathbb{Q}$,$a\ \overline{\in}\ H$.显然 $a\neq0$.又 $H\neq\{0\}$,从而 $\exists b\in H$,$b\neq0$.因 $\mathbb{Q}$ 是有理数集,故方程 $ax=b$ 在 $\mathbb{Q}$ 中有解 $x=\dfrac{n}{m}$($\dfrac{n}{m}$是有理数,m,n 都是非零整数),从而

$a \cdot \frac{n}{m}=b$. 因 $b \in H$，m 是整数，H 是子加群，故 $an=mb \in H$. 所以，虽 $a \overline{\in} H$，$a \in \mathbb{Q}$，但 $\exists$ 非零整数 n，使得 $an \in H$. 于是

$$\overline{H} = \left\{ h + ka \,\middle|\, h \in H, k \in \mathbb{Z} \right\}$$

是 $\mathbb{Q}$ 的子加群. 事实上，由 $0=0+0a \in \overline{H}$，$\overline{H} \neq \varnothing$. 显然 $\overline{H} \subset \mathbb{Q}$. $\forall x, y \in \overline{H}$，$x=h_1+k_1a$，$y=h_2+k_2a$，有 $-y=-h_2+(-k_2)a$，$x-y=x+(-y)=(h_1-h_2)+(k_1-k_2)a \in \overline{H}$. 所以 $\overline{H}$ 是 $\mathbb{Q}$ 的子加群.

$\overline{H} \neq \mathbb{Q}$. 这是因为，由 $n \neq 0$，$\exists \frac{a}{n} \in \mathbb{Q}$，但 $\frac{a}{n} \overline{\in} \overline{H}$. 不然，若 $\frac{a}{n} \in \overline{H}$，则 $\frac{a}{n}=h+ka$，其中 $h \in H$，$k \in \mathbb{Z}$. 因此，由 $an \in H$，H 是子加群，故 $a=nh+kan \in H$. 此与 $a \overline{\in} H$ 矛盾，所以 $\frac{a}{n} \overline{\in} \overline{H}$，即 $\overline{H} \neq \mathbb{Q}$.

因 $a=0+1a \in \overline{H}$，但 $a \overline{\in} H$，故 $\overline{H} \neq H$.

因 $\forall h \in H$，$h=h+0a \in \overline{H}$，故 $H \subset \overline{H}$.

命题得证. 下面证明环 $\mathbb{Q}$ 没有最大理想.

由环 $\mathbb{Q}$ 的代数运算知加群 $\mathbb{Q}$ 的任意子加群都是环 $\mathbb{Q}$ 的理想. 设 $\mathfrak{A}$ 是加群 $\mathbb{Q}$ 的任一子加群，即 $\mathfrak{A}$ 是环 $\mathbb{Q}$ 的任一理想. 且 $\mathfrak{A} \neq \mathbb{Q}$，$\mathfrak{A} \neq \{0\}$. 根据前面命题知，$\exists$ 加群 $\mathbb{Q}$ 的子加群 $\mathfrak{B}$. 即 $\exists$ 环 $\mathbb{Q}$ 的理想 $\mathfrak{B}$，$\mathfrak{B} \neq \mathbb{Q}$，$\mathfrak{B} \neq \mathfrak{A}$，但 $\mathfrak{B} \supset \mathfrak{A}$. 即存在中间理想 $\mathfrak{B}$，使 $\mathfrak{A} \subsetneqq \mathfrak{B} \subsetneqq \mathbb{Q}$. 所以 $\mathfrak{A}$ 不是 $\mathbb{Q}$ 的最大理想. 若 $\mathfrak{A}=\{0\}$. 显然存在中间理想 (2)，使 $\{0\} \subsetneqq (2) \subsetneqq \mathbb{Q}$，所以 $\{0\}$ 不是 $\mathbb{Q}$ 的最大理想. 于是环 $\mathbb{Q}$ 没有最大理想.

利用前面命题，还可证明：$R=\left\{ (a,b) \,\middle|\, a,b \in \mathbb{Q} \right\}$ 对于

$$(a,b) = (c,d) \Leftrightarrow a = c,\ b = d,$$

$$(a,b) + (c,d) = (a+c, b+d),$$

$$(a,b)(c,d) = (0, ac)$$

作成一个环，则环 R 没有最大理想(证明略).

5)　未必唯一. 如 (2)，(3) 都是整数环 $\mathbb{Z}$ 的最大理想.

2. 设 $\mathbb{Z}$ 是整数环，p 是正整数，证明：

p 是素数 $\Leftrightarrow$ (p) 是 $\mathbb{Z}$ 的最大理想[①].

证　$(\Rightarrow)$　设 $\mathfrak{A}$ 是 $\mathbb{Z}$ 的任一理想，$\mathfrak{A} \supset (p)$，$\mathfrak{A} \neq (p)$. 已知 $\mathbb{Z}$ 的任一理想都是主理想(见第十二章，三，2)，从而 $\mathfrak{A}=(a)$ (a 是正整数)，即 $(a) \supsetneqq (p)$. 因此 $p \in (a)$，即 $a \mid p$. 因 p 是素数，故 $a=p$ 或 1. 若 $a=p$，则 $(a)=(p)$，矛盾. 因此 $a=1$，于是 $\mathfrak{A}=(a)=(1)=\mathbb{Z}$. 所以 (p) 是 $\mathbb{Z}$ 的最大理想.(另一证法：因 p 是素数，故由第十章，一，2，$\mathbb{Z}_p$ 是域. 由第十二章，一，7，$\mathbb{Z}/(p)=\mathbb{Z}_p$，从而 $\mathbb{Z}/(p)$ 是域. 又 $\mathbb{Z}$ 是有单位元的交换环，所以 (p) 是 $\mathbb{Z}$ 的最大理想[②].)

$(\Leftarrow)$　不然，若正整数 p 不是素数，又 $p \neq 1$. 否则，若 $p=1$，则 $(p)=(1)=\mathbb{Z}$ 不是 $\mathbb{Z}$ 的最大理想，与已知矛盾，从而 $p \neq 1$. 于是 p 是合数. 可设 $p=n_1n_2$，$1<n_i<p$，$i=1,2$. 考察 (n_2)：因 $p=n_1n_2$，故 $p \in (n_2)$，从而 $(p) \subset (n_2)$. 因 $n_2<p$，故 $p \nmid n_2$，即 $n_2 \overline{\in} (p)$，从而 $(p) \neq$

---

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 117. 例 1.

② 同上 118. 定理.

(n_2). 因 $n_2>1$，故 $n_2\nmid 1$，即 $1\notin(n_2)$，但 $1\in\mathbb{Z}$，从而 $(n_2)\neq\mathbb{Z}$. 所以 $(p)\subsetneqq(n_2)\subsetneqq\mathbb{Z}$. 此与 (p) 是 $\mathbb{Z}$ 的最大理想矛盾. 于是 p 是素数.

注 1) 因素数有无穷多个，故 $\mathbb{Z}$ 有无穷多个最大理想：(2)，(3)，(5)，(7)，…

因 $(4)\subsetneqq(2)\subsetneqq\mathbb{Z}$，故(4)不是 $\mathbb{Z}$ 的最大理想.

2) (2)是 $\mathbb{Z}$ 的最大理想，但(2)不是有理数环 $\mathbb{Q}$ 的最大理想. 因 $\mathbb{Q}$ 是有单位元的交换环，2 是 $\mathbb{Q}$ 的可逆元，故由第十二章，一，4，9)，$(2)=\mathbb{Q}$. 所以(2)不是 $\mathbb{Q}$ 的最大理想.

3. 关于命题：若有单位元($\neq 0$)的交换环 R 除了零理想同单位理想以外没有其他的理想，那么 R 一定是一个域[①].

1) 若 R 为非交换环时，即：如果 R 是一个有单位元($\neq 0$)的环，且 R 只有零理想与单位理想，那么 R 是否为除环？

2) 条件 R 有单位元不等于零用在何处？

3) 该命题的逆命题："设 R 是一个域，则 R 是一个有单位元($\neq 0$)的交换环，且 R 除零理想与单位理想外没有其他的理想"是否成立？

答 1) R 未必为除环. 见第十三章，二，4.

2) 因 R 有单位元不等于零，故 R 至少包含一个不等于零的元，这样才符合除环定义中的条件.

3) 由域的定义可知该命题的逆命题成立[②]，从而有：设 R 是有单位元的交换环，且 $R\neq\{0\}$，则

$$R\text{ 是域}\Leftrightarrow R\text{ 只有当然理想.}$$

4. 利用一个有单位元的交换环的最大理想来造域的方法是什么？

答 我们有个重要定理：设 R 是有单位元的交换环，$\mathfrak{A}$ 是 R 的理想，则

$$R/\mathfrak{A}\text{ 是域}\Leftrightarrow\mathfrak{A}\text{ 是 }R\text{ 的最大理想}^{③}.$$

于是，若 $\mathfrak{A}$ 是有单位元的交换环 R 的最大理想，则利用 $\mathfrak{A}$ 可造出一个域 $R/\mathfrak{A}$.

注 1) 该定理中的必要性可把条件减弱．即：设 $\mathfrak{A}$ 是环 R 的理想，若 $R/\mathfrak{A}$ 是除环，则 $\mathfrak{A}$ 是 R 的最大理想. 也就是说，去掉环 R 有单位元、可交换的条件后，仍可得结论. 事实上，因 $R/\mathfrak{A}$ 是除环，故 $R/\mathfrak{A}\neq\{[0]\}$，即 $R\neq\mathfrak{A}$. 且 $R/\mathfrak{A}$ 只有零理想和单位理想. 所以 $\mathfrak{A}$ 是 R 的最大理想[④].

2) 该定理的充分性中，条件环 R 有单位元不可去掉，见第十三章，二，3. 环 R 可交换这一条件显然不能去掉.

3) 设 $\mathfrak{A}$ 是环 R 的最大理想，R 不是交换环，则 $R/\mathfrak{A}$ 连除环也未必是. 例，设 F 是域，$n\geqslant 2$，则由第十三章，二，4，$M_n(F)$ 没有真理想，从而零理想 $\{0\}$ 是 $M_n(F)$ 的最大理想. $M_n(F)$ 不是交换环. 因 $M_n(F)$ 有零因子(见第九章，三，7，2))，故 $M_n(F)/\{0\}(\cong M_n(F))$ 也有零因子，所以 $M_n(F)/\{0\}$ 不是除环.

4) 有单位元的交换环 R 的最大理想 $\mathfrak{A}$ 是使剩余类环 $R/\mathfrak{A}$ 成为域的理想，而域是最强

---

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 118. 引理 2.

② 同上. 110. 定理 1.

③ 同上. 118. 定理.

④ 同上. 117. 引理 1.

的环. 由此可见最大理想在理想中的特殊功用.

5. 商域(也称分式域或比域)的定义是什么?

答　设

1)　Q是一个域;

2)　Q以环R为子环;

3)　$Q=\left\{\frac{a}{b}\middle|a,b\in R,b\neq 0\right\}$,其中$\frac{a}{b}=ab^{-1}=b^{-1}a$,

则称Q为R的一个商域.

注　1)　在条件3)中,$a,b\in R\subset Q,b\neq 0$,因$Q$是域,故$\exists b^{-1}\in Q$(当然$b^{-1}$未必$\in R$). 由$Q$的乘法运算,有$\frac{a}{b}=ab^{-1}=b^{-1}a\in Q$,从而必有$\left\{\frac{a}{b}\ \middle|\ a,b\in R,b\neq 0\right\}\subset Q$. 但反之,未必成立. 例,实数域$\mathbb{R}$以整数环$\mathbb{Z}$为子环,且有$\left\{\frac{a}{b}\middle|a,b\in\mathbb{Z},b\neq 0\right\}$(即有理数集)$\subset\mathbb{R}$. 但$\mathbb{R}\neq\left\{\frac{a}{b}\middle|a,b\in\mathbb{Z},b\neq 0\right\}$,从而实数域不是整数环的商域. 说明了以环$R$为子环的域未必是$R$的商域.

2)　有理数域是整数环的一个商域. 由此还可看出,以整数环为子环的域包含整数环的商域:有理数域. 因为有理数域是最小数域.

3)　讨论环R的商域Q,即把环R扩充成域Q,可使R的非零元在Q中有逆元. 这样,既方便,又扩大了研究范围.

6. 关于定理1:

R是无零因子的交换环$\Leftrightarrow\exists$域Q,使得R是Q的子环①.

1)　证明中,为何先将$R=\{0\}$除外,假定R至少有两个元?

2)　证明中,取定$q(\neq 0)\in R$,作环$R_0=\left\{\text{所有类}\left[\frac{qa}{q}\right]\middle|a\in R\right\}$,使$R_0$是$Q_0$的子环,且$R_0\cong R$. 显然$\left[\frac{qa}{q}\right]=\left[\frac{a}{1}\right]$. 那么为何不把$R_0$写成形式更为简单的$\left\{\left[\frac{a}{1}\right]\ \middle|\ a\in R\right\}$? 再者,将$R_0$写成$\left\{\left[\frac{a}{q}\right]\middle|a\in R\right\}$行不行? 其中$q$是$R$中取定的一个非零元.

3)　域Q中的元呈何形式?

答　1)　因环$R\neq\{0\}$,故集

$$A=\left\{\text{符号}\frac{a}{b}\middle|a,b\in R,b\neq 0\right\}\neq\varnothing$$

才能保证下面的证明是有意义的.

2)　因为R中未必有单位元1,所以无从谈起$\left[\frac{qa}{q}\right]=\left[\frac{a}{1}\right]$,$R_0$也就不能写成$\left\{\left[\frac{a}{1}\right]\middle|a\in R\right\}$.

若将R_0写成$\left\{\left[\frac{a}{q}\right]\middle|a\in R\right\}$,则$\forall\left[\frac{a}{q}\right],\left[\frac{b}{q}\right]\in R_0$,$\left[\frac{a}{q}\right]\left[\frac{b}{q}\right]=\left[\frac{ab}{q^2}\right]$未必在$R_0$中,即

① 张禾瑞. 近世代数基础. 北京:高等教育出版社,1978. 119. 定理1.

不能保证 R_0 对于 Q_0 的乘法封闭，当然更谈不上 R_0 是 Q_0 的子环了. 所以 R_0 不能写成$\left\{\left[\frac{a}{q}\right] \middle| a\in R\right\}$.

3） $Q=\left\{a\in R;类\left[\frac{a}{b}\right]\in Q_0-R_0\right\}$.

7. 详细证明定理 2：设 R 是无零因子的交换环，$R\neq\{0\}$，则定理 1 证明中给出的域 $Q=\left\{a\in R;类\left[\frac{a}{b}\right]\in Q_0-R_0\right\}$，即为$\left\{\frac{a}{b}\middle| a,b\in R,b\neq 0\right\}$，其中$\frac{a}{b}=ab^{-1}=b^{-1}a$[①].

证　我们由 6 题中的定理 1 的证明，知$Q_0\overset{\psi}{\cong}Q$. 其中域 $Q_0=\left\{类\left[\frac{a}{b}\right]\middle|\frac{a}{b}\in A,a,b\in R,b\neq 0\right\}$，而 Q_0 的子环 $R_0=\left\{类\left[\frac{qa}{q}\right]\middle| a\in R\right\}$，其中 q 是 R 中取定的一个非零元.

$\forall\alpha\in Q$，因 ψ 是满射，故 $\exists\left[\frac{a}{b}\right]\in Q_0$，使得 ψ：$\left[\frac{a}{b}\right]\to\alpha$. 又 $\exists\left[\frac{qa}{q}\right],\left[\frac{qb}{q}\right]\in R_0\subset Q_0$，使得 ψ：$\left[\frac{qa}{q}\right]\to a,\left[\frac{qb}{q}\right]\to b$. 因 ψ 是同构映射，故 ψ：$\left[\frac{qb}{q}\right]^{-1}\to b^{-1},\left[\frac{qa}{q}\right]\left[\frac{qb}{q}\right]^{-1}\to ab^{-1}$. 因

$$\left[\frac{qa}{q}\right]\left[\frac{qb}{q}\right]^{-1}=\left[\frac{qa}{q}\right]\left[\frac{q}{qb}\right]=\left[\frac{q^2a}{q^2b}\right]=\left[\frac{a}{b}\right].$$

又 ψ 是映射，故 $\alpha=ab^{-1}=\frac{a}{b}\in\left\{\frac{a}{b}\middle| a,b\in R,b\neq 0\right\}$，所以 $Q\subset\left\{\frac{a}{b}\middle| a,b\in R,b\neq 0\right\}$.

反之，$\forall\frac{a}{b}\in\left\{\frac{a}{b}\middle| a,b\in R,b\neq 0\right\}$. 因 $a,b\in R\subset Q$，Q 是域，又 $b\neq 0$，即 $\exists b^{-1}\in Q$，故$\frac{a}{b}=ab^{-1}\in Q$，所以$\left\{\frac{a}{b}\middle| a,b\in R,b\neq 0\right\}\subset Q$.

于是 $Q=\left\{\frac{a}{b}\middle| a,b\in R,b\neq 0\right\}$.

8. 6 题中的定理 1 和 7 题中的定理 2 的意义为何？

答　由定理 1,2 知：若 R 是一个至少有两个元的无零因子的交换环，则必 $\exists$ 域 Q，使得 R 是 Q 的子环且 $Q=\left\{\frac{a}{b}\middle| a,b\in R,b\neq 0\right\}$. 因此 Q 是 R 的商域. 这就说明了 R 的商域必存在. 即任意一个至少有两个元的无零因子的交换环都可嵌入到商域 Q 中.

实际上造环的商域的方法就是从整数环 $\mathbb{Z}$ 造有理数域 $\mathbb{Q}$ 的方法. $\mathbb{Q}$ 就是 $\mathbb{Z}$ 的一个商域.

9. 详细证明定理：设 R 与 R' 都是至少含两个元的无零因子的交换环，且 $R\overset{\phi}{\cong}R'$，则 R 的商域 $Q\cong R'$的商域 Q' [②].

证　$\forall\frac{a}{b}\in Q$，规定

$$\psi:\frac{a}{b}\to\frac{\phi(a)}{\phi(b)}.$$

则 ψ 是 Q 与 Q'间的一个同构映射，事实上，

---

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 123. 定理 2.

② 同上. 124. 定理 4.

1）　$\forall \frac{a}{b}\in Q$，因ϕ是映射，故$\exists\, \phi(a),\phi(b)\in R'$. 因$b\neq 0$，$\phi$是单射，故$\phi(b)\neq 0$，从而$\exists \frac{\phi(a)}{\phi(b)}\in Q'$，使得$\psi: \frac{a}{b}\rightarrow \frac{\phi(a)}{\phi(b)}$. 若$\frac{a}{b}=\frac{c}{d}$，则必$\frac{\phi(a)}{\phi(b)}=\frac{\phi(c)}{\phi(d)}$. 因$\frac{a}{b}=\frac{c}{d}$，故$ad=bc$. 又$\phi$保持运算，从而$\phi(a)\phi(d)=\phi(b)\phi(c)$. 因$b\neq 0$，$d\neq 0$，$\phi$是单射，故$\phi(b)\neq 0$. $\phi(d)\neq 0$. 于是$\frac{\phi(a)}{\phi(b)}=\frac{\phi(c)}{\phi(d)}$，即象唯一. 所以$\psi$是映射.

2）　$\forall \frac{a'}{b'}\in Q'$. 因$\phi$是满射，故$\exists\, a,b\in R$，使得$\phi(a)=a'$，$\phi(b)=b'$，因$b'\neq 0$，$\phi$是同态满射，故$b\neq 0$，从而$\exists \frac{a}{b}\in Q$，使得$\psi: \frac{a}{b}\rightarrow \frac{\phi(a)}{\phi(b)}=\frac{a'}{b'}$. 所以$\psi$是满射.

3）　$\forall \frac{a}{b},\frac{c}{d}\in Q$. 设$\phi(a)=a'$，$\phi(b)=b'$，$\phi(c)=c'$，$\phi(d)=d'$. 若$\frac{a'}{b'}=\frac{c'}{d'}$，即$a'd'=b'c'$，从而$\phi(a)\phi(d)=\phi(b)\phi(c)$，于是$\phi(ad)=\phi(bc)$. 因$\phi$是单射，故$ad=bc$. 因$b\neq 0$，$d\neq 0$，故$\frac{a}{b}=\frac{c}{d}$. 所以$\psi$是单射.

4）
$$\forall\ \frac{a}{b},\frac{c}{d}\in Q,\psi:\ \frac{a}{b}\rightarrow \frac{\phi(a)}{\phi(b)},\frac{c}{d}\rightarrow \frac{\phi(c)}{\phi(b)}.$$
于是
$$\psi:\ \frac{a}{b}+\frac{c}{d}=\frac{ad+cb}{bd}\rightarrow \frac{\phi(a)\,\phi(d)+\phi(c)\,\phi(b)}{\phi(b)\,\phi(d)}=\frac{\phi(a)}{\phi(b)}+\frac{\phi(c)}{\phi(d)},$$
$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}\rightarrow \frac{\phi(a)\,\phi(c)}{\phi(b)\,\phi(d)}=\frac{\phi(a)}{\phi(b)}\cdot\frac{\phi(c)}{\phi(d)}.$$
所以$Q\overset{\psi}{\cong}Q'$.

注　取$R'=R$，当然$R\cong R$，从而设Q与Q'都是环R的商域，则$Q\cong Q'$. 即在同构观点下，环R的商域唯一.

二、典型问题分析

1. 假定R是由所有复数$a+bi$(a,b是整数)所作成的环. 证明：$R/(1+i)$是一个域.

证一　$R\sim R/(1+i)$①. 因R是有单位元$1(\neq 0)$的交换环，故$R/(1+i)$也是有单位元$[1](\neq[0])$的交换环，由第十二章，二，9，$R/(1+i)=\{[0],[1]\}$. 从而$R/(1+i)$只有零理想和单位理想. 由第十三章，一，3，$R/(1+i)$是域.

证二　R是一个有单位元的交换环. 下面证明$(1+i)$是R的最大理想. 设$\mathfrak{A}$是R的一个理想，且$R\supset\mathfrak{A}\supset(1+i)$，$\mathfrak{A}\neq(1+i)$. 往证$\mathfrak{A}=R$. $\exists\, a+bi\in\mathfrak{A}$，但$a+bi\,\overline{\in}\,(1+i)$，从而$a$与$b$奇偶相反. 于是$a+1$与$b$奇偶相同. 由此$a+1+bi\in(1+i)\subset\mathfrak{A}$. 因$\mathfrak{A}$是加群，故$(a+1+bi)-(a+bi)=1\in\mathfrak{A}$，又$\mathfrak{A}$是理想，从而$\mathfrak{A}=(1)=R$. 所以$(1+i)$是$R$的最大理想. 由第十三章，一，4，$R/(1+i)$是域.

证三　由第十二章，二，9，$R/(1+i)=\{[0],[1]\}(\neq\{[0]\})$是一个有单位元$[1]$的交换环，且$R/(1+i)$中非零元$[1]$有逆元$[1]$. 所以由域定义，$R/(1+i)$是域.

---

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 114. 定理1.

证四 由第十二章，二，9，$R/(1+\mathrm{i})=\{[0],[1]\}$是交换环，又$R/(1+\mathrm{i})-\{[0]\}=\{[1]\}$对于乘法来说是一个群，从而$R/(1+\mathrm{i})$是域.

证五 由第十二章，二，9，$R/(1+\mathrm{i})=\{[0],[1]\}$，于是$R/(1+\mathrm{i})$与模2的剩余类环$\mathbb{Z}_2$同构.又2是素数，从而$\mathbb{Z}_2$是域.所以$R/(1+\mathrm{i})$也是域.

2. 我们看环R上的一个一元多项式环$R[x]$.当R是整数环时，$R[x]$的理想(x)是不是最大理想？当R是有理数域的时候，情形如何？

解一 1) 当R是整数环时，(x)不是$R[x]$的最大理想.事实上，$R[x]$是一个有单位元的交换环，从而

$$(x)=\{xf(x)\mid f(x)\in R[x]\}=\{c_1x+c_2x^2+\cdots+c_mx^m\mid c_i\in R,m\text{ 是正整数}\},$$

$$(2,x)=\{2a_0+a_1x+\cdots+a_nx^n\mid a_i\in R,n\text{ 是非负整数}\}^{①},$$

$$R[x]=\{b_0+b_1x+\cdots+b_nx^n\mid b_i\in R,n\text{ 是非负整数}\}.$$

于是$(x)\subset(2,x)\subset R[x]$.因$2\in(2,x)$，但$2\overline{\in}(x)$，故$(2,x)\neq(x)$.因$1\in R[x]$，但$1\overline{\in}(2,x)$，故$(2,x)\neq R[x]$（或因$(2,x)$不是主理想，从而$(2,x)\neq(x)$，$(2,x)\neq(1)=R[x]$）.所以$(x)$不是$R[x]$的最大理想.

2) 当R是有理数域时，(x)是$R[x]$的最大理想.事实上，设$\mathfrak{A}$是$R[x]$的一个理想，且$R[x]\supset\mathfrak{A}\supset(x)$，而$\mathfrak{A}\neq(x)$.往证$\mathfrak{A}=R[x]$.$\exists\, g(x)=b_0+b_1x+\cdots+b_nx^n\in\mathfrak{A}$，而$g(x)\overline{\in}(x)$，因此$b_0\neq0$，$b_0\in R$.但$h(x)=b_1x+\cdots+b_nx^n\in(x)\subset\mathfrak{A}$，由$\mathfrak{A}$是加群，$b_0=g(x)-h(x)\in\mathfrak{A}$.因$R$是有理数域，$b_0(\neq0)\in R$，故$\exists\, b_0^{-1}\in R\subset R[x]$.因$\mathfrak{A}$是$R[x]$的理想，故$b_0^{-1}b_0=1\in\mathfrak{A}$，于是$\mathfrak{A}=(1)=R[x]$.所以$(x)$是$R[x]$的最大理想.

解二 $R[x]$是一个有单位元的交换环.由第十二章，三，6，3)的证明知

$$R[x]/(x)=\{[f(x)]\mid f(x)\in R[x]\}=\{[a]\mid a\in R\}\cong R.$$

当R是整数环时，R不是域，从而$R[x]/(x)$也不是域.由第十三章，一，4，(x)不是$R[x]$的最大理想.当R是有理数域时，$R[x]/(x)$是域，由第十三章，一，4，(x)是$R[x]$的最大理想.

注 1) 一般来说，若F是域，则(x)是$F[x]$的最大理想.但(x)不是$F[x,y]$的最大理想.事实上，$F[x,y]$是一个有单位元的交换环，从而

$$(x,y)=\{xh(x,y)+yk(x,y)\mid h(x,y),k(x,y)\in F[x,y]\}.$$

即(x,y)由常数项为0的所有F上的x,y的多项式组成.于是$F[x,y]\supset(x,y)\supset(x)$.因$1\in F[x,y]$，但$1\overline{\in}(x,y)$，故$(x,y)\neq F[x,y]$.因$y\in(x,y)$，但$y\overline{\in}(x)$，故$(x,y)\neq(x)$.所以$(x)$不是$F[x,y]$的最大理想.

还可如下证明：$\phi:f(x,y)\to f(0,y)$是$F[x,y]$到$F[y]$的同态满射.$\ker\phi=(x)=\{xf(x,y)\mid f(x,y)\in F[x,y]\}$，从而$F[x,y]/(x)\cong F[y]$.因$F[y]$不是域，故$F[x,y]/(x)$也不是域，由第十三章，一，4，$(x)$不是$F[x,y]$的最大理想.

2) (x)不是$\mathbb{Z}[x]$的最大理想，但我们有

$$(x,n)(n\in\mathbb{Z})\text{是}\mathbb{Z}[x]\text{的最大理想}\Leftrightarrow n\text{是素数}.$$

① 张禾瑞.近世代数基础.北京：高等教育出版社，1978.112.例3.

证明如下：$\phi: f(x) \to [f(0)]$是环$\mathbb{Z}[x]$到环$\mathbb{Z}_n$的同态满射. 事实上，

① $\forall f(x)\in\mathbb{Z}[x]$, $\exists| f(0)\in\mathbb{Z}$，从而$\exists|[f(0)]=f(0)+(n)\in\mathbb{Z}_n$，使得$\phi(f(x))=[f(0)]$.

② $\forall [a]\in\mathbb{Z}_n$，$\exists a\in\mathbb{Z}\subset\mathbb{Z}[x]$，使得$\phi(a)=[a]$.

③ $\forall f(x), g(x)\in\mathbb{Z}[x]$，

$$\phi(f(x)\dot{+}g(x))=[f(0)\dot{+}g(0)]=[f(0)]\dot{+}[g(0)]=\phi(f(x))\dot{+}\phi(g(x)).$$

所以$\mathbb{Z}[x]\overset{\phi}{\sim}\mathbb{Z}_n$. 又 $\ker\phi=(x,n)$. 事实上，

$$(x,n)=\left\{xf(x)+ng(x)\,\middle|\,f(x),g(x)\in\mathbb{Z}[x]\right\}$$
$$=\left\{na_0+a_1x+\cdots+a_mx^m\,\middle|\,a_i\in\mathbb{Z}, m\text{ 是非负整数}\right\}.$$

$\forall f(x)\in\ker\phi$, $\phi(f(x))=[f(0)]=[0]$，从而$n\,|\,f(0)$，即 $f(x)$的常数项是 n 的倍数，从而 $f(x)\in(x,n)$，所以 $\ker\phi\subset(x,n)$. 反之，$\forall na_0+a_1x+\cdots+a_mx^m\in(x,n)$，

$$\phi(na_0+a_1x+\cdots+a_mx^m)=[na_0]=[0],$$

从而 $na_0+a_1x+\cdots+a_mx^m\in\ker\phi$，所以$(x,n)\subset\ker\phi$. 于是 $\ker\phi=(x,n)$. 因此$\mathbb{Z}[x]/(x,n)\cong\mathbb{Z}_n$，这里$\mathbb{Z}[x]$是一个有单位元的交换环. 我们有，

(x,n)是$\mathbb{Z}[x]$的最大理数$\xLeftrightarrow{\text{由第十三章，一，4}}\mathbb{Z}[x]/(x,n)$是域$\Leftrightarrow\mathbb{Z}_n$是域$\Leftrightarrow n$是素数.

3. 我们看所有偶数作成的环 R. 证明：(4)是 R 的最大理想，但 $R/(4)$不是一个域.

证一　因 R 是无单位元的交换环，故

$$(4)=\left\{4r+4n\,\middle|\,r\in R, n\in\mathbb{Z}\right\}=\left\{4(r+n)\,\middle|\,r\in R, n\in\mathbb{Z}\right\}=\left\{4k\,\middle|\,k\in\mathbb{Z}\right\}.$$

设$\mathfrak{A}$是 R 的一个理想且$R\supset\mathfrak{A}\supsetneq(4)$，则$\exists a\in\mathfrak{A}$, $a\,\overline{\in}\,(4)$，即 $4\nmid a$，从而$\exists q, r\in\mathbb{Z}$，使得 $a=4q+r$，但 $0<r<4$. 因 a 是偶数，故 r 是偶数，只能 $r=2$. 因 $4q\in(4)\subset\mathfrak{A}$，$\mathfrak{A}$是加群，故 $2=r=a-4q\in\mathfrak{A}$. $\forall 2n\in R$，由 $2\in\mathfrak{A}$，$\mathfrak{A}$是加群，有 $2n\in\mathfrak{A}$，于是 $R\subset\mathfrak{A}$. 因此$\mathfrak{A}=R$. 所以(4)是 R 的最大理想.

由第十二章，三，5，$R/(4)=\{[0],[2]\}$，其中$[0]$是 $R/(4)$的零元. 因$[2][2]=[4]=[0]\neq[2]$，故$[2]$不是 $R/(4)$的单位元，即 $R/(4)$无单位元. 所以 $R/(4)$不是域.

证二　设$\mathfrak{A}$是 R 的一个理想，且 $R\supsetneq\mathfrak{A}\supset(4)$，则 $2\,\overline{\in}\,\mathfrak{A}$. 这是因为：若 $2\in\mathfrak{A}$，而$\mathfrak{A}$是加群，则 $R=\mathfrak{A}$，矛盾. 下面证明$\mathfrak{A}=(4)$. $\forall a\in\mathfrak{A}$，$\exists q, r\in\mathbb{Z}$，使得 $a=4q+r$, $0\leqslant r<4$. 因 $4q\in(4)\subset\mathfrak{A}$，$\mathfrak{A}$是加群，故 $r=a-4q\in\mathfrak{A}$. 但 $2\,\overline{\in}\,\mathfrak{A}$，从而 $r\neq2$. 又 a 与 $4q$ 都是偶数，r 也就只能是偶数，因此 $r=0$. 即 $a=4q\in(4)$，于是$\mathfrak{A}\subset(4)$，又$(4)\subset\mathfrak{A}$，即$\mathfrak{A}=(4)$. 所以(4)是 R 的最大理想.

因 $R/(4)$有零因子$[2]$，故 $R/(4)$不是域.

证三　$(4)=\left\{4k\,\middle|\,k\in\mathbb{Z}\right\}=[0]\in R/(4)$. $\forall a\in R$, $a\,\overline{\in}\,(4)$，于是$\exists q\in\mathbb{Z}$，使得 $a=4q+2$，从而 $a-2=4q\in(4)$. 即$[a]=[2]$，因此 $a\in[2]$. 所以 $R/(4)=\{[0],[2]\}$，从而 $R/(4)$只有零理想和单位理想. 于是(4)是 R 的最大理想.

因 $R/(4)$无单位元，故 $R/(4)$不是域.

注　一般来说，设 $2\mathbb{Z}$ 是偶数环，p 是素数，则$(2p)$是 $2\mathbb{Z}$ 的最大理想. 当素数 $p\neq2$ 时，$2\mathbb{Z}/(2p)$是域.

事实上，因 $2\mathbb{Z}$ 是无单位元的交换环，故

$$(2p)=\left\{2pr+2pn\,\middle|\,r\in2\mathbb{Z}, n\in\mathbb{Z}\right\}=\left\{2p(r+n)\,\middle|\,r\in2\mathbb{Z}, n\in\mathbb{Z}\right\}=\left\{2pk\,\middle|\,k\in\mathbb{Z}\right\}.$$

设$\mathfrak{A}$是 $2\mathbb{Z}$ 的一个理想，且 $2\mathbb{Z}\supset\mathfrak{A}\supsetneq(2p)$，则$\exists 2a\in\mathfrak{A}$, $a\in\mathbb{Z}$, $2a\,\overline{\in}\,(2p)$，从而 $2p\nmid 2a$，

即 $p\nmid a$. 又 p 是素数,于是 a,p 互素. $\exists u,v\in\mathbb{Z}$,使得 $ua+vp=1$,即 $2=u(2a)+v(2p)$. 因 $2a\in\mathfrak{A}$,$u\in\mathbb{Z}$,$\mathfrak{A}$是加群,故 $u(2a)\in\mathfrak{A}$. 又因 $2p\in(2p)\subset\mathfrak{A}$,$v\in\mathbb{Z}$,$\mathfrak{A}$是加群,故 $v(2p)\in\mathfrak{A}$. 因$\mathfrak{A}$是加群,故 $2=u(2a)+v(2p)\in\mathfrak{A}$. 从而 $\forall 2r\in 2\mathbb{Z}$,有 $2r\in\mathfrak{A}$,即 $2\mathbb{Z}\subset\mathfrak{A}$. 又$\mathfrak{A}\subset 2\mathbb{Z}$,于是$\mathfrak{A}=2\mathbb{Z}$. 所以$(2p)$是 $2\mathbb{Z}$ 的最大理想.

当素数 $p\neq 2$ 时,环 $2\mathbb{Z}/(2p)$无零因子. 事实上,$\forall a+(2p),b+(2p)\in 2\mathbb{Z}/(2p)$,若$[a+(2p)][b+(2p)]=(2p)=[0]$,即 $ab+(2p)=(2p)$,则 $ab\in(2p)$. 于是 $2p\mid ab$,又 $p\mid 2p$. 从而 $p\mid ab$. 因 p 是素数,故 $p\mid a$ 或 $p\mid b$,即 $a=q_1p$ 或 $b=q_2p$. 因 a,b 是偶数,$p\neq 2$,故 q_1,q_2 是偶数. 可分别记为 $2s_1,2s_2,s_1,s_2\in\mathbb{Z}$,即 $a=s_1(2p)$或 $b=s_2(2p)$. 因此 $2p\mid a$ 或 $2p\mid b$,即 $a\in(2p)$或 $b\in(2p)$,从而 $a+(2p)=(2p)=[0]$或 $b+(2p)=(2p)=[0]$. 所以 $2\mathbb{Z}/(2p)$无零因子.

因 $2\mathbb{Z}$ 是交换环,故 $2\mathbb{Z}/(2p)$也是交换环.

$2\mathbb{Z}/(2p)$有单位元$[p+1]$. 这是因为:$\forall[2n]\in 2\mathbb{Z}/(2p)$,有$[2n][p+1]=(2n+(2p))(p+1+(2p))=2np+2n+(2p)=2n+(2p)=[2n]$. 因 p 是奇素数,故 $p+1\in 2\mathbb{Z}$,$[p+1]\in 2\mathbb{Z}/(2p)$.

$$\begin{aligned}2\mathbb{Z}/(2p)&=\{2n+(2p)\mid n\in\mathbb{Z}\}\\&=\{2\cdot 0+(2p),2\cdot 1+(2p),2\cdot 2+(2p),\cdots,2(p-1)+(2p)\},\end{aligned}$$

从而 $2\mathbb{Z}/(2p)$恰含 p 个元,是个有限环.

根据第十章,二,3,$2\mathbb{Z}/(2p)$是个域.

例 (6)是 $2\mathbb{Z}$ 的一个最大理想且 $2\mathbb{Z}/(6)$是域. 实际上,$2\mathbb{Z}/(6)\cong\mathbb{Z}/(3)=\mathbb{Z}_3$.

4. 我们看有理数域 F 上的全部 2×2 矩阵环 F_{22}. 证明:F_{22}只有零理想同单位理想,但不是一个除环.

证一 设$\mathfrak{A}$是 F_{22}的理想且$\mathfrak{A}\neq\{0\}$. 往证$\mathfrak{A}=F_{22}$. $\exists\begin{pmatrix}a&b\\c&d\end{pmatrix}(\neq 0)\in\mathfrak{A}$,不妨设 $a\neq 0$,则由$\mathfrak{A}$是理想,

$$\begin{pmatrix}\frac{1}{a}&0\\0&0\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}1&0\\0&0\end{pmatrix}=\begin{pmatrix}1&0\\0&0\end{pmatrix}\in\mathfrak{A},\begin{pmatrix}0&0\\\frac{1}{a}&0\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&1\end{pmatrix}\in\mathfrak{A}.$$

$\mathfrak{A}$当然是加群,从而$\begin{pmatrix}1&0\\0&0\end{pmatrix}+\begin{pmatrix}0&0\\0&1\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}\in\mathfrak{A}$. 因 F_{22}的单位元$\begin{pmatrix}1&0\\0&1\end{pmatrix}$在理想$\mathfrak{A}$中,故$\mathfrak{A}=F_{22}$. 所以 F_{22}只有零理想同单位理想.

因$\begin{pmatrix}1&0\\0&0\end{pmatrix}(\neq 0)\in F_{22}$,而$\begin{pmatrix}1&0\\0&0\end{pmatrix}$在 F_{22}中无逆元,故 F_{22}不是除环.

证二 设$\mathfrak{A}$是 F_{22}的非零的理想,则$\exists\begin{pmatrix}a&b\\c&d\end{pmatrix}(\neq 0)\in\mathfrak{A}$. 由《高等代数》知,

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}\xrightarrow{\text{初等变换}}\begin{pmatrix}1&0\\0&l\end{pmatrix},$$

其中 $l=1$ 或 0. 而对$\begin{pmatrix}a&b\\c&d\end{pmatrix}$施行初等变换化为标准形$\begin{pmatrix}1&0\\0&l\end{pmatrix}$,相当于用 F_{22}中若干个初等

矩阵 $E_1,E_2,\cdots,E_t$ 左或右乘$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$得$\begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix}$，即

$$E_1\cdots E_s\begin{pmatrix} a & b \\ c & d \end{pmatrix}E_{s+1}\cdots E_t = \begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix}.$$

因$\mathfrak{A}$是理想，故$\begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix}\in\mathfrak{A}$. 当 $l=1$（即秩$\begin{pmatrix} a & b \\ c & d \end{pmatrix}=2$）时，$\mathfrak{A}=F_{22}$；当 $l=0$（即秩$\begin{pmatrix} a & b \\ c & d \end{pmatrix}=1$）时，有$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\in\mathfrak{A}$，再由$\mathfrak{A}$是理想，$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\in\mathfrak{A}$，$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}+\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\in\mathfrak{A}$，于是$\mathfrak{A}=F_{22}$. 所以 F_{22} 只有当然理想.

取$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}(\neq 0)$，$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}(\neq 0)\in F_{22}$，但$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$，从而 F_{22} 有零因子. 所以 F_{22} 不是除环.

注　1)　由第十二章，二，6，F_{22} 有真左（右）理想. 本命题说明 F_{22} 无真理想.

2)　本命题还说明了：第十三章，一，3 中的 R 如果是一个有单位元 $1(\neq 0)$ 的非交换环，虽 R 只有当然理想，但 R 却未必是除环.

3)　一般来说，设 R 是除环，则 R 上 n 阶全矩阵环 $M_n(R)$ 只有零理想同单位理想.

事实上，设$\mathfrak{A}$是 $M_n(R)$ 的非零的理想，则 $\exists\,(a_{ij})(\neq 0)\in\mathfrak{A}$. 设 $a_{kl}(\in R)\neq 0$，其中 $1\leqslant k,l\leqslant n$. 因 R 是除环，故 $\exists\, a_{kl}^{-1}\in R$. 令 E_{ij} 表示第 i 行第 j 列位置的元为单位元 1 而其余位置的元都是零的 n 阶矩阵，$i,j=1,2,\cdots,n$. 因 $a_{kl}^{-1}E_{ik}$，$E_{lj}\in M_n(R)$，$\mathfrak{A}$是理想，故

$$a_{kl}^{-1}E_{ik}(a_{ij})E_{lj} = i\text{行}\begin{pmatrix} & \overset{k\text{列}}{\vdots} & \\ \cdots & a_{kl}^{-1} & \cdots \\ & \vdots & \end{pmatrix}(a_{ij})E_{lj} = i\text{行}\begin{pmatrix} & \overset{l\text{列}}{\vdots} & \\ a_{kl}^{-1}a_{k1}\cdots & a_{kl}^{-1}a_{kl}\cdots a_{kl}^{-1}a_{kn} \\ & \vdots & \end{pmatrix}E_{lj}$$

$$= i\text{行}\begin{pmatrix} & \vdots & \\ a_{kl}^{-1}a_{k1}\cdots & 1 & \cdots a_{kl}^{-1}a_{kn} \\ & \underset{l\text{列}}{\vdots} & \end{pmatrix}\begin{pmatrix} & \vdots & \\ \cdots & 1 & \cdots \\ & \underset{j\text{列}}{\vdots} & \end{pmatrix} = i\text{行}\begin{pmatrix} & \vdots & \\ \cdots & 1 & \cdots \\ & \underset{j\text{列}}{\vdots} & \end{pmatrix} = E_{ij}\in\mathfrak{A}.$$

$i,j=1,2,\cdots,n$. $\forall\,(x_{ij})\in M_n(R)$，因 $x_{ij}E_{ii}\in M_n(R)$，$\mathfrak{A}$是理想，故

$$(x_{ij}) = \sum_{i=1}^{n}\sum_{j=1}^{n}x_{ij}E_{ij} = \sum_{i=1}^{n}\sum_{j=1}^{n}(x_{ij}E_{ii})E_{ij}\in\mathfrak{A},$$

从而 $M_n(R)\subset\mathfrak{A}$. 又$\mathfrak{A}\subset M_n(R)$，于是$\mathfrak{A}=M_n(R)$. 所以 $M_n(R)$ 只有当然理想.

5. 证明：一个域 F 是它自己的商域.

证一　设 Q 是 F 的商域，当然 $F\subset Q$. 下面证明 $Q\subset F$. $\forall\, x\in Q$，$x=\dfrac{a}{b}$，其中 $a,b\in F$，$b\neq 0$. 因 F 是域，故 $b^{-1}\in F$，从而 $x=\dfrac{a}{b}=ab^{-1}\in F$，于是 $Q\subset F$. 所以 $F=Q$.

证二　已知 F 是一个域，F 以环 F 为子环，因此由商域定义，只需证明 $F=\left\{\dfrac{a}{b}\,\middle|\, a,b\in F,\ b\neq 0\right\}$. $\forall\, x\in F$，因域 F 有单位元 1，故 $x=x1=x1^{-1}=\dfrac{x}{1}\in$

$\left\{\frac{a}{b}\ \middle|\ a,b\in F,b\neq0\right\}$，从而 $F\subset\left\{\frac{a}{b}\ \middle|\ a,b\in F,b\neq0\right\}$；反之，$\forall\ \frac{a}{b}\in\left\{\frac{a}{b}\ \middle|\ a,b\in F,b\neq0\right\}$，因 F 是域，故 $\frac{a}{b}=ab^{-1}\in F$，从而 $\left\{\frac{a}{b}\ \middle|\ a,b\in F,b\neq0\right\}$. 于是 $F=\left\{\frac{a}{b}\ \middle|\ a,b\in F,b\neq0\right\}$. 所以根据商域定义，域 F 是 F 的商域.

证三 域 F 是一个有两个以上的元的环，F 是一个包含 F 的域. 则 F 包含 F 的一个商域 Q[①]，即 $F\supset Q$. 又由商域定义，$Q\supset F$. 所以 $F=Q$.

6. 详细证明下面命题：假定 R 是一个有两个以上的元的环，F 是一个包含 R 的域，那么 F 包含 R 的一个商域.[②]

证 作集

$$\overline{Q}=\left\{\frac{a}{b}\middle|a,b\in R,b\neq0\right\},$$

其中 $\frac{a}{b}=ab^{-1}=b^{-1}a\in F$.

1) $\overline{Q}$ 是 F 的子域，从而 $\overline{Q}$ 对于 F 的代数运算来说作成一个域. 事实上，

$\forall\ \frac{a}{b}\in\overline{Q}$，有 $\frac{a}{b}=ab^{-1}$，$a,b\in R,b\neq0$. 因 $R\subset F$，故 $a,b\in F$. 又因 F 是域，故 $b^{-1}\in F$，$\frac{a}{b}=ab^{-1}\in F$，即 $\overline{Q}\subset F$.

因环 R 至少有两个元，故 $\exists\, b(\neq0)\in R,0\in R$，从而 $\exists\, 0=0b^{-1}=\frac{0}{b}\in\overline{Q}$，即 $\overline{Q}\neq\varnothing$.

又域 F 中的单位元 $1=bb^{-1}=\frac{b}{b}\in\overline{Q}$，从而 $\overline{Q}$ 含不等于零的元 1.

$$\forall\ \frac{a}{b},\frac{c}{d}\in\overline{Q},a,b,c,d\in R,b\neq0,d\neq0,$$

$$\frac{a}{b}-\frac{c}{d}=ab^{-1}-cd^{-1}=add^{-1}b^{-1}-cbb^{-1}d^{-1}=ad(bd)^{-1}-cb(bd)^{-1}$$

$$=(ad-cb)(bd)^{-1}=\frac{ad-cb}{bd}.$$

因 $ad-cb,bd\in R$，又 $b,d\in F,b\neq0,d\neq0$，域 F 无零因子，即 $bd\neq0$，故 $\frac{a}{b}-\frac{c}{d}=\frac{ad-cb}{bd}\in\overline{Q}$.

$\forall\ \frac{a}{b},\frac{c}{d}\in\overline{Q},\frac{c}{d}\neq0$，即 $c\neq0$，且 $a,b,c,d\in R,b\neq0,d\neq0$，类似地有

$$\frac{a}{b}\left(\frac{c}{d}\right)^{-1}=(ab^{-1})(cd^{-1})^{-1}=ab^{-1}dc^{-1}=ad(bc)^{-1}=\frac{ad}{bc}\in\overline{Q}.$$

所以 $\overline{Q}$ 是 F 的子域.

2) $\overline{Q}$ 以 R 为子环. 事实上，$\forall\, a\in R$，取 $b(\neq0)\in R$，有

$$a=a(bb^{-1})=(ab)b^{-1}=\frac{ab}{b}\in\overline{Q},$$

从而 $R\subset\overline{Q}$. 又因 R 是 F 的子环，故 R 对于 F 的代数运算，也就是 $\overline{Q}$ 的代数运算来说作成一个环. 所以 R 是 $\overline{Q}$ 的子环.

---

①② 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 124. 定理 3.

再由 $\overline{Q}$ 中元的形式，于是依商域定义，$\overline{Q}$ 是 R 的一个商域且 $F\supset\overline{Q}$.

注　环 R 的商域是包含 R 的所有的域中的最小的域.

三、讲与练

1. 判断以下各命题是否正确.

1）设环 $R\overset{\phi}{\sim}$ 环 $\overline{R}$. 若 $\mathfrak{A}$ 是 R 的最大理想，则 $\mathfrak{A}$ 在 ϕ 下的象 $\phi(\mathfrak{A})$ 也是 $\overline{R}$ 的最大理想.

2）设环 $R\overset{\phi}{\sim}$ 环 $\overline{R}$. 若 $\overline{\mathfrak{A}}$ 是 $\overline{R}$ 的最大理想，则 $\overline{\mathfrak{A}}$ 在 ϕ 下的逆象 $\phi^{-1}(\overline{\mathfrak{A}})$ 也是 R 的最大理想.

3）设 Q 是环 R 的商域，则 R 的任一非零元在 Q 中都有逆元.

4）任一有单位元的无零因子环必包含在一个商域中.

解　1）不正确. 例，取 R 为整数环，$\overline{R}=\{0\}$，则 ϕ: $n\to 0$ 是 R 到 $\overline{R}$ 的一个同态满射. $\mathfrak{A}=(2)$ 是 R 的最大理想. $\phi(\mathfrak{A})=\{0\}$ 是 $\overline{R}$ 的理想，但不是 $\overline{R}$ 的最大理想. 又例，取 $R=\mathbb{Z}$，$\overline{R}=\mathbb{Z}_3$，则 ϕ: $n\to[n]$ 是 $\mathbb{Z}$ 到 $\mathbb{Z}_3$ 的一个同态满射. $\mathfrak{A}=(2)$ 是 $\mathbb{Z}$ 的最大理想，但 $\phi(\mathfrak{A})=\mathbb{Z}_3$ 不是 $\mathbb{Z}_3$ 的最大理想.

2）不正确.

例，取 $R=\mathbb{Z}$，$\overline{R}=\{0,1\}$. $\forall_n\in\mathbb{Z}$，ϕ: $n(\neq 0)\to 1, 0\to 0$ 是 $\mathbb{Z}$ 到 $\overline{R}$ 的一个同态满射. $\overline{\mathfrak{A}}=\{0\}$ 是 $\overline{R}$ 的最大理想，但 $\phi^{-1}(\overline{\mathfrak{A}})=\{0\}$ 不是 $\mathbb{Z}$ 的最大理想.

3）正确. 因为商域 Q 是以 R 为子环的域.

4）不正确. 因为非交换环没有商域. 例，四元数除环不存在商域.

2. 下面各理想 $\mathfrak{A}$ 是否为环 R 的最大理想，$R/\mathfrak{A}$ 是不是域?

1）$R=\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$，$\mathfrak{A}=(\sqrt{2})$.

2）$R=\left\{\dfrac{a}{b}\in\mathbb{Q}\;\middle|\; a,b\in\mathbb{Z}, p\nmid b\right\}$，$p$ 是素数，$\mathfrak{A}=(p)$.

3）$R=\mathbb{Z}[\mathrm{i}]=\{a+b\mathrm{i}\mid a,b\in\mathbb{Z}\}$，$\mathfrak{A}=(2+2\mathrm{i})$.

4）$R=\mathbb{Z}_6$，$\mathfrak{A}=\{[0],[2],[4]\}$.

5）$R=\mathbb{Z}_{12}$，$\mathfrak{A}=\{[0],[3],[6],[9]\}$.

6）$R=\mathbb{Z}_{pq}$，p,q 是不同的素数，$\mathfrak{A}=([p])$.

7）$R=\mathbb{Z}[x]$，$\mathfrak{A}=(2)$.

8）$R=\mathbb{Q}[x]$，$\mathfrak{A}=(x-1)$.

9）R 是定义在闭区间 $[0,1]$ 上的所有实函数的集作成的环，即 $[0,1]$ 上的全实函数环（见第九章，三，9，注 1）），$\mathfrak{A}=\{f\in R\mid f(0)=0\}$.

解　1）$(\sqrt{2})$ 是 $\mathbb{Z}[\sqrt{2}]$ 的最大理想. 事实上，因 $\mathbb{Z}[\sqrt{2}]$ 是有单位元的交换环，故

$$(\sqrt{2})=\{(a+b\sqrt{2})\sqrt{2}\mid a,b\in\mathbb{Z}\}=\{2b+a\sqrt{2}\mid 2b\in 2\mathbb{Z}, a\in\mathbb{Z}\}\neq\mathbb{Z}[\sqrt{2}].$$

设 $\mathfrak{B}$ 是 $\mathbb{Z}[\sqrt{2}]$ 的理想，且 $\mathbb{Z}[\sqrt{2}]\supset\mathfrak{B}\supsetneqq(\sqrt{2})$，则 $\exists\, a+b\sqrt{2}\in\mathfrak{B}$. 但 $a+b\sqrt{2}\,\overline{\in}\,(\sqrt{2})$，从而 a 是奇数，于是 $a-1$ 是偶数.

由$\mathfrak{B}$是加群，$1=(a+b\sqrt{2})-[(a-1)+b\sqrt{2}]\in\mathfrak{B}$，因此$\mathfrak{B}=(1)=\mathbb{Z}[\sqrt{2}]$.

所以$(\sqrt{2})$是$\mathbb{Z}[\sqrt{2}]$的最大理想.

因$\mathbb{Z}[\sqrt{2}]$是有单位元的交换环，故由第十三章，一，4，$\mathbb{Z}[\sqrt{2}]/(\sqrt{2})$是域. 实际上，

$$\phi: a+b\sqrt{2}\to \begin{matrix}[0],\ a\text{ 是偶数；}\\ [1],\ a\text{ 是奇数.}\end{matrix}$$

ϕ是$\mathbb{Z}[\sqrt{2}]$到$\mathbb{Z}_2$的一个同态满射，$\ker\phi=(\sqrt{2})$，从而$\mathbb{Z}[\sqrt{2}]/(\sqrt{2})\cong\mathbb{Z}_2$.

2) (p)是R的最大理想. 事实上，因R是有单位元的交换环，故

$$(p)=\left\{\frac{pa}{b}\ \middle|\ pa\in p\mathbb{Z},b\in\mathbb{Z},p\nmid b\right\}\neq R.$$

设$\mathfrak{B}$是R的理想且$R\supset\mathfrak{B}\supsetneqq(p)$，则$\exists\ \frac{a}{b}\in\mathfrak{B}(a,b\in\mathbb{Z},p\nmid b)$，但$\frac{a}{b}\overline{\in}(p)$，即$a$不是$p$的整数倍，从而$p\nmid a$. 由$p$是素数，$a$与$p$互素，于是$\exists\ u,v\in\mathbb{Z}$，使得$ua+vp=1$. 因$\mathfrak{B}$是$R$的理想，$b=\frac{b}{1}\in R$，$\frac{a}{b}\in\mathfrak{B}$，故$b\cdot\frac{a}{b}=a\in\mathfrak{B}$. 又$p\in(p)\subset\mathfrak{B}$，因此$1=ua+vp\in\mathfrak{B}$，即$\mathfrak{B}=(1)=R$. 所以$(p)$是$R$的最大理想. 于是由第十三章，一，4，$R/(p)$是域.

3) $(2+2\mathrm{i})$不是$\mathbb{Z}[\mathrm{i}]$的最大理想.

事实上，$\exists\ \mathbb{Z}[\mathrm{i}]$的理想$(1+\mathrm{i})=\{a+b\mathrm{i}\mid a,b\in\mathbb{Z},a,b\text{同奇偶}\}$（见第十二章，二，9），因$\mathrm{i}\in\mathbb{Z}[\mathrm{i}]$，但$\mathrm{i}\overline{\in}(1+\mathrm{i})$，故$(1+\mathrm{i})\neq\mathbb{Z}[\mathrm{i}]$.

因$1+\mathrm{i}\in(1+\mathrm{i})$，但$1+\mathrm{i}\overline{\in}(2+2\mathrm{i})$，故$(1+\mathrm{i})\neq(2+2\mathrm{i})$. 但$(1+\mathrm{i})\supset(2+2\mathrm{i})$.

所以$(2+2\mathrm{i})$不是$\mathbb{Z}[\mathrm{i}]$的最大理想. 因此由第十三章，一，4，$\mathbb{Z}[\mathrm{i}]/(2+2\mathrm{i})$不是域.

4) $\mathfrak{A}$是$\mathbb{Z}_6$的最大理想. $\mathbb{Z}_6/\mathfrak{A}$是域.

5) $\mathfrak{A}$是$\mathbb{Z}_{12}$的最大理想. $\mathbb{Z}_{12}/\mathfrak{A}$是域.

6) $([p])$是$\mathbb{Z}_{pq}$的最大理想. $\mathbb{Z}_{pq}/([p])$是域.

7) (2)不是$\mathbb{Z}[x]$的最大理想. 事实上，$\exists\ \mathbb{Z}[x]$的理想$(2,x)=\{2a_0+a_1x+\cdots+a_nx^n\mid a_i\in\mathbb{Z},n\geqslant0\}$，使得$\mathbb{Z}[x]\supsetneqq(2,x)\supsetneqq(2)$. 所以$(2)$不是$\mathbb{Z}[x]$的最大理想. $\mathbb{Z}[x]/(2)$不是域.

8) $(x-1)$是$\mathbb{Q}[x]$的最大理想. 由第十二章，三，6，注可知. $\mathbb{Q}[x]/(x-1)$是域.

9) $\mathfrak{A}$是R的最大理想. $R/\mathfrak{A}$是域.

实际上，$\phi: f\to f(0)$是R到实数域$\mathbb{R}$的一个同态满射，$\ker\phi=\mathfrak{A}$，从而$R/\mathfrak{A}\cong\mathbb{R}$.

3. 设R是有单位元$1(\neq0)$的交换环，证明下面各命题等价.

1) R是域.

2) 零理想$\{0\}$是R的最大理想.

3) R没有真理想.

4) 任意一个环R到非零环$\overline{R}$的同态满射都是单射.

证 1) $\Rightarrow$ 2)，2) $\Rightarrow$ 3)，显然. 参看第十三章，一，1，3).

3) ⇒ 4)　设ϕ是环 R 到非零环 $\overline{R}$ 的任一同态满射. 则 $\ker\phi$是 R 的一个理想[①]. 假设 $\ker\phi=R$,则 $\forall a\in R,\phi(a)=\overline{0}\in\overline{R}$,其中 $\overline{0}$ 是 $\overline{R}$ 的零元. 但 $\overline{R}$ 是非零环,从而 $\exists\,\overline{b}\in\overline{R},\overline{b}\neq\overline{0}$. 可是 $\overline{b}$ 在ϕ下无逆象,此与ϕ是满射矛盾,于是 $\ker\phi\neq R$. 已知 R 无真理想,所以 $\ker\phi=\{0\}$. 由第十二章,二,8,ϕ是 R 到 $\overline{R}$ 的单射.

4) ⇒ 1)　只需证明 R 中任一非零元都可逆. 假设 $a\in R$,a 不是可逆元,依第十二章,一,4,9),$(a)\neq R$,从而 $R/(a)$是一个非零环. ϕ: $x\to[x]=x+(a)$是 R 到 $R/(a)$的一个同态满射,$\ker\phi=(a)$. 由已知条件,ϕ是单射,于是ϕ是同构映射. 由第十二章,二,8,$\ker\phi=\{0\}$. 因此$(a)=\{0\}$,即 $a=0$. 所以 R 中任一非零元都是可逆元. 又已知 R 是有单位元 $1(\neq 0)$的交换环,从而 R 是域.

4. 试判断下列各域 Q 是否为环 R 的商域.

1)　R 是偶数环 $2\mathbb{Z}$,Q 是有理数域$\mathbb{Q}$.

2)　$R=\left\{\dfrac{m}{2^n}\,\middle|\, m\in\mathbb{Z},n\geqslant 0 \text{ 的整数}\right\}$. Q 是有理数域$\mathbb{Q}$.

3)　$R=\left\{\dfrac{m}{n}\,\middle|\, m,n\in\mathbb{Z},p\nmid n\right\}$,$p$ 是素数. Q 是有理数域$\mathbb{Q}$.

4)　$R=\mathbb{Z}[\mathrm{i}]=\{a+b\mathrm{i}\mid a,b\in\mathbb{Z}\}$,$Q=\mathbb{Q}(\mathrm{i})=\{x+y\mathrm{i}\mid x,y\in\mathbb{Q}\}$.

5)　$R=\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$,$Q=\mathbb{Q}(\sqrt{2})=\{x+y\sqrt{2}\mid x,y\in\mathbb{Q}\}$.

6)　$R=\{a+b\sqrt{3}\mid a,b\in 2\mathbb{Z}\}$,$Q=\mathbb{Q}(\sqrt{3})=\{x+y\sqrt{3}\mid x,y\in\mathbb{Q}\}$.

7)　R 是域 F 上的一元多项式环 $F[x]$,$Q=F(x)=\left\{\dfrac{f(x)}{g(x)}\,\middle|\, f(x),g(x)\in F[x],g(x)\neq 0\right\}$.

8)　$R=\mathbb{Z}_6$,$Q=\mathbb{Z}_3$.

解　1)　易证 $2\mathbb{Z}$ 是$\mathbb{Q}$的子环.

$$\mathbb{Q}=\left\{\frac{a}{b}\,\middle|\, a,b\in\mathbb{Z},b\neq 0\right\}=\left\{\frac{2a}{2b},2a,2b\in 2\mathbb{Z},2b\neq 0\right\},$$

所以$\mathbb{Q}$是 $2\mathbb{Z}$ 的一个商域.

2)　易证 R 是$\mathbb{Q}$的子环.(见第九章,四,1,7)). $\forall\dfrac{a}{b}\in\mathbb{Q},a,b\in\mathbb{Z},b\neq 0$,

$$\frac{a}{b}=\frac{2^n m}{2^{n_1}m_1}=\frac{m}{2^{n_1}}\cdot\frac{2^n}{m_1}=\frac{m}{2^{n_1}}\left(\frac{m_1}{2^n}\right)^{-1},$$

其中 $m,m_1\in\mathbb{Z},m_1\neq 0$,$n$ 与 n_1 是大于或等于零的整数,所以$\mathbb{Q}$是 R 的一个商域.

3)　易证 R 是$\mathbb{Q}$的子环. $\forall\dfrac{a}{b}\in\mathbb{Q},a,b\in\mathbb{Z},b\neq 0$. 当$\dfrac{a}{b}\neq 0$ 时,

$$\frac{a}{b}=\frac{p^n c}{p^{n_1}d}=\frac{p^n}{d}\cdot\frac{c}{p^{n_1}}=\frac{p^n}{d}\left(\frac{p^{n_1}}{c}\right)^{-1},$$

其中 $p\nmid c,p\nmid d,c\neq 0,c,d\in\mathbb{Z}$. 当$\dfrac{a}{b}=0$ 时,

$$\frac{a}{b}=\frac{a}{1}\cdot\frac{1}{b}=\frac{a}{1}\left(\frac{b}{1}\right)^{-1}.$$

① 张禾瑞. 近世代数基础. 北京:高等教育出版社,1978. 114. 定理 2.

所以$\mathbb{Q}$是R的一个商域.

4) 易证$\mathbb{Z}[\mathrm{i}]$是$\mathbb{Q}(\mathrm{i})$的一个子环. $\forall x+y\mathrm{i}\in\mathbb{Q}(\mathrm{i}),x,y\in\mathbb{Q}$,可令$x=\frac{a}{b},y=\frac{c}{d},a,b,c,d\in\mathbb{Z},b\neq0,d\neq0$,

$$x+y\mathrm{i}=\frac{a}{b}+\frac{c}{d}\mathrm{i}=\frac{ad+cb\mathrm{i}}{bd}=(ad+cb\mathrm{i})(bd+0\mathrm{i})^{-1}.$$

所以$\mathbb{Q}(\mathrm{i})$是$\mathbb{Z}[\mathrm{i}]$的一个商域.

5) 易证$\mathbb{Z}[\sqrt{2}]$是$\mathbb{Q}(\sqrt{2})$的一个子环. 与上面题4)类似地可证明$\mathbb{Q}(\sqrt{2})$是$\mathbb{Z}[\sqrt{2}]$的一个商域.

6) 易证R是$\mathbb{Q}(\sqrt{3})$的一个子环. $\forall x+y\sqrt{3}\in\mathbb{Q}(\sqrt{3}),x,y\in\mathbb{Q}$. 设$x=\frac{a}{b},y=\frac{c}{d},a,b,c,d\in\mathbb{Z},b\neq0,d\neq0$.

$$x+y\sqrt{3}=\frac{a}{b}+\frac{c}{d}\sqrt{3}=\frac{ad+cb\sqrt{3}}{bd}=\frac{2ad+2cb\sqrt{3}}{2bd}=(2ad+2cb\sqrt{3})(2bd+0\sqrt{3})^{-1}.$$

所以$\mathbb{Q}(\sqrt{3})$是R的一个商域.

7) 显然$F(x)$是$F[x]$的一个商域. 称$F(x)$为域F上的一元有理分式域. $F(x)$的运算类似于分式的加法与乘法.

注 ① $F[x]$的商域$F(x)$是包含域F和未定元x的最小域. 事实上,$F\subset F[x],x\in F[x]$,又$F[x]\subset F(x)$,从而$F\subset F(x),x\in F(x)$. 设P是包含F和x的任一域,因$F[x]$是包含F和x的最小子环,故$F[x]\subset P$. $\forall\frac{f(x)}{g(x)}\in F(x),f(x),g(x)(\neq0)\in F[x]$,因$F[x]\subset P$,故$f(x),g(x)(\neq0)\in P$. 因$P$是域,故$\frac{f(x)}{g(x)}=f(x)(g(x))^{-1}\in P$,于是$F(x)\subset P$. 所以$F(x)$是含$F$和$x$的最小域.

② 类似地,设F是域,则

$$F(x_1,x_2,\cdots,x_n)=\left\{\frac{f(x_1,x_2,\cdots,x_n)}{g(x_1,x_2,\cdots,x_n)}\,\middle|\,f(x_1,x_2,\cdots,x_n),g(x_1,x_2,\cdots,x_n)(\neq0)\in F[x_1,x_2,\cdots,x_n]\right\}$$

是$F[x_1,x_2,\cdots,x_n]$的一个商域. 称之为域F上的n元有理分式域.

8) 因$\mathbb{Z}_6$有零因子$[2],[3]$,故$\mathbb{Z}_6$没有商域,所以$\mathbb{Z}_3$不是$\mathbb{Z}_6$的商域.

5. 证明:

1) 整环$R(\neq\{0\})$与其商域Q有相同的特征.

2) 设Q是环R的商域,$\forall\frac{a}{b},\frac{c}{d}\in Q$,其中$a,b,c,d\in R,\frac{c}{d}\neq0,b\neq0,d\neq0$,当然$c\neq0$,则$\frac{a}{b}/\frac{c}{d}=\frac{ad}{bc}$.

证 1) 因R与Q的单位元分别对于加法来说的阶是R与Q的特征,又由第十一章,一,5,1),R与Q的单位元一样,故$\mathrm{ch}\,R=\mathrm{ch}\,Q$.

2)

$$\frac{a}{b}/\frac{c}{d}=\frac{ab^{-1}}{cd^{-1}}=ab^{-1}(cd^{-1})^{-1}=ab^{-1}dc^{-1}=adc^{-1}b^{-1}=ad(bc)^{-1}=\frac{ad}{bc}.$$

四、思考问题

1. 求出整数环$\mathbb{Z}$的包含理想(30)的全部最大理想.

2. 设$R(\neq\{0\})$是整环,Q是R的一个商域.证明:R上未定元x也是Q上未定元.

3. 设a,b是整环$R(\neq\{0\})$的两个元,且有互素的两个整数m,n,使$a^m=b^m,a^n=b^n$.证明:$a=b$.

第十四章　素元、唯一分解环、主理想环

一、基本问题问答

1. 证明：在整环 I 里，

1）　$a|b, b|c \Rightarrow a|c$.

2）　$a|b, a|c \Rightarrow a|b\pm c$.

3）　$a|b \Rightarrow \forall c\in I, a|bc$.

4）　若 $c(\neq 0)\in I$，则 $a|b \Leftrightarrow ac|bc$.

5）　$a|b \Leftrightarrow a|\varepsilon b$，其中 ε 是 I 的单位．

证　利用整除定义易证 1)～4)．下面证 5)．

$(\Rightarrow)$　$a|b \Rightarrow \exists u\in I$，使得 $b=au$. 设 ε 是 I 的单位，因 I 是交换环，故 $\varepsilon b=\varepsilon au=a(\varepsilon u)$，从而 $a|\varepsilon b$.

$(\Leftarrow)$　$a|\varepsilon b \Rightarrow \exists v\in I$，使得 $\varepsilon b=av$. 因 ε 是 I 的单位，故 $\exists \varepsilon^{-1}\in I$，使得 $\varepsilon^{-1}\varepsilon b=\varepsilon^{-1}av$. 因 I 是交换环，故 $b=a(\varepsilon^{-1}v)$，从而 $a|b$.

2. 试判断下面各命题是否正确．在整环 I 里，

1）　零元 0 是 I 的单位．

2）　a 是 I 的单位 $\Leftrightarrow a$ 是 I 的单位元．

3）　设 $a=bc$，则 a 是单位 $\Leftrightarrow b,c$ 都是单位．

4）　设 $I\neq\{0\}$，则

$$I\text{ 是域} \Leftrightarrow I\text{ 中每个非零元都是单位}.$$

5）　I 里必有单位 1 与 -1.

6）　I 至少有两个不同的单位 1 与 -1.

7）　ε 是 I 的单位 $\Leftrightarrow -\varepsilon$ 是 I 的单位．

答　1）　不正确．当 $I\neq\{0\}$时，0 不是 I 的单位．但当 $I=\{0\}$时，0 是 I 的单位．

2）　$(\Rightarrow)$　不正确．例，-1 是整数环 $\mathbb{Z}$ 的单位，但 -1 不是 $\mathbb{Z}$ 的单位元．$(\Leftarrow)$　正确．

3）　正确．事实上，$(\Rightarrow)$　a 是单位 $\Rightarrow \exists a^{-1}\in I$，使得 $aa^{-1}=b\,ca^{-1}\Rightarrow b(ca^{-1})=1$，其中 $ca^{-1}\in I$. 所以 b 是单位．同理 c 是单位．$(\Leftarrow)$　自证．

注　该命题说明单位的因子仍是单位，从而单位只有平凡因子，无真因子．单位的相伴元仍是单位．

4）　正确．由定义直接可知．

5)　正确．显然．

6)　不正确．例，零环$\{0\}$只有 1 个单位 0. $I=\{0,1\}$对于

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

作成一个整环．I 只有 1 个单位 1.

7)正确．事实上，($\Rightarrow$)　ε 是单位 $\Rightarrow \exists \varepsilon^{-1}\in I$，使得 $\varepsilon\varepsilon^{-1}=1 \Rightarrow (-\varepsilon)(-\varepsilon^{-1})=1$，其中 $-\varepsilon^{-1}\in I$，所以$-\varepsilon$ 是单位．($\Leftarrow$)　$-\varepsilon$ 是单位，由必要性$-(-\varepsilon)=\varepsilon$ 是单位．

3. 证明：

1)　设 $a,b\in$整环 I，则

$$a\,\big|\,b,\ b\,\big|\,a \Leftrightarrow b\text{ 是 }a\text{ 的相伴元}.$$

2)　整环 I 的全体单位的集 U 对于 I 的乘法作成一个群．

证　1)　($\Rightarrow$)　$b\neq 0$ 时，由 $a\,|\,b,b\,|\,a$，$\exists c,c'\in I$，使得 $b=ac,a=bc'$，于是 $b=bcc'$. 因 $b\neq 0$，I 中消去律成立，故 $1=cc'$，从而 c 与 c'都是单位．所以 b 是 a 的相伴元．$b=0$ 时，由 $b\,|\,a$知，$\exists c'\in I$，使得 $a=bc'=0$，于是 $b=a=1a$，从而 b 是 a 的相伴元．

($\Leftarrow$)　因 b 是 a 的相伴元，故$\exists I$ 的单位ε，使得$b=\varepsilon a$，从而 $a\,|\,b$. 因ε 是单位，故$\exists\varepsilon^{-1}\in I$，使得 $a=\varepsilon^{-1}b$，从而 $b\,|\,a$.

2)　由群的定义可证．

注　1)　由该命题 1)知

$$b\text{ 是 }a\text{ 的相伴元}\Leftrightarrow a\text{ 是 }b\text{ 的相伴元}.$$

即 a 与 b 互为相伴元，从而称 a,b 相伴或 b,a 相伴．

2)　$U=\{\varepsilon\in I\,|\,\varepsilon\text{ 是单位}\}$不是整环 $I(\neq\{0\})$的子群．这是因为，U 对于 I 的乘法作成一个群，但 I 对于 I 的乘法不能作成群(见第九章，一，9，3)). I 对于 I 的加法作成一个加群，而$\bigcup$对于 I 的加法却不能作成群．例，整数环 $\mathbb{Z}$ 的全部单位的集 $U=\{1,-1\}$. 因 $1+(-1)=0\,\overline{\in}\,U$，故 U 对于 $\mathbb{Z}$ 的加法不封闭，U 对于 $\mathbb{Z}$ 的加法不能作成群．所以 U 不是 $\mathbb{Z}$ 的子群．

3)　将整环 I 的条件减弱为含单位元 1 的环 R，命题 2)仍成立．即含单位元 1 的环 R 的全体可逆元的集对于 R 的乘法作成一个群．由此显然得知，除环 R 的全体非零元(即全体可逆元)的集 R^* 对于 R 的乘法作成一个群，R^* 就是除环 R 的乘群①．我们再给出两个例子.

例 1　当 $n\geqslant 2$ 时，数域 F 上 n 阶矩阵的集 $M_n(F)$作成一个有单位元的环．$M_n(F)$的全体可逆元恰是 F 上全体 n 阶可逆矩阵，而 F 上全体 n 阶可逆矩阵的集 $GL_n(F)$对于 $M_n(F)$的乘法作成一个群(见第五章，二，6).

例 2　$\mathbb{Z}_6$的全体可逆元的集$\{[1],[5]\}$对于$\mathbb{Z}_6$的乘法作成一个群．

4)　整环 I 的全体非零元的集对于 I 的乘法未必作成群．例，$\mathbb{Z}$ 的全体非零元的集对于 $\mathbb{Z}$ 的乘法不能作成群．

---

①　张禾瑞．近世代数基础．北京：高等教育出版社，1978. 90. (b).

4. 证明:在整环 I 里,

1) $a,0$ 相伴 $\Leftrightarrow a=0$.

2) $a,1$ 相伴 $\Leftrightarrow a$ 是单位.

3) 若 a,b 相伴,则

① $c \mid a \Leftrightarrow c \mid b$.

② $a \mid c \Leftrightarrow b \mid c$.

4) 若 a,a' 相伴且 b,b' 相伴,则 $ab,a'b'$ 相伴.

5) 若 $ab,a'b'$ 相伴,a,a' 相伴且 $a\neq 0$,则 b,b' 相伴.

证 1) 显然由定义可知.

2) 易证.

注 由该命题可知

$$\varepsilon \text{ 是单位} \Leftrightarrow \varepsilon \mid 1.$$

$$\varepsilon \text{ 是单位} \Leftrightarrow \varepsilon \text{ 整除 } I \text{ 中每一个元}.$$

3) 读者自证.

4) 因 a,a' 相伴,b,b' 相伴,故 $\exists I$ 的单位 ε,ε',使得 $a=\varepsilon a'$,$b=\varepsilon' b'$,从而 $ab=\varepsilon a'\varepsilon' b'=(\varepsilon\varepsilon')(a'b')$. 其中 $\varepsilon\varepsilon'$ 是 I 的单位,所以 $ab,a'b'$ 相伴.

5) 利用相伴定义,I 中消去律成立,$a\neq 0$,可证.

5. 证明:在整环 I 中,若 a 不是素元,则 a 的相伴元也不是素元.

证一 (反证法)假设 a 的相伴元 εa(ε 是单位)是素元,因 $\varepsilon^{-1}\varepsilon a=a$ 是素元 εa 的相伴元,故素元 εa 的相伴元 a 也是一个素元[①],此与已知矛盾. 所以 a 的相伴元不是素元.

证二 1) $a=0$ 时,显然 0 的相伴元 0 不是素元.

2) a 是单位时,显然单位 a 的相伴元是单位而不是素元.

3) $a\neq 0$ 且 $a\neq$ 单位时,因 a 不是素元,故 a 有真因子 $b\in I$,使得 $a=cb$,其中 $c\in I$. 设 ε 是单位,则 $\varepsilon a=\varepsilon cb$,从而 $b \mid \varepsilon a$. 又 $b\neq$ 单位,$b\neq \varepsilon a$ 的相伴元,因此 b 是 εa 的真因子,所以 εa 不是素元.

6. 关于命题:设 $a(\neq 0)\in$ 整环 I,则

$$a \text{ 有真因子} \Leftrightarrow a=bc,\ b,\ c\in I,\ b,\ c \text{ 都不是单位}^{②}.$$

证明中,条件 $a=0$ 用在何处? 该命题的逆否命题是什么?

答 1) 在充分性证明中:设 $a=bc$,b,c 都不是单位. 假定 b 不是 a 的真因子,又 $b\neq$ 单位,则 $b=\varepsilon a$,ε 是单位,从而 $a=\varepsilon ac=a(\varepsilon c)$. 利用条件 $a\neq 0$,由整环 I 中消去律成立,才有 $1=\varepsilon c$,于是 $c=$ 单位,矛盾. 所以 b 是 a 的真因子.

2) 该命题的逆否命题是:设 $a(\neq 0)\in$ 整环 I,则

$$a \text{ 没有真因子} \Leftrightarrow \forall b,c\in I,\ a=bc,\ \text{其中 } b \text{ 或 } c \text{ 是单位}.$$

注 2)可换个说法:设 $p(\neq 0)\in$ 整环 I,$p\neq$ 单位,则

$$p \text{ 是 } I \text{ 的素元} \Leftrightarrow \forall b,c\in I,\ p=bc,\ \text{其中 } b \text{ 或 } c \text{ 是单位}.$$

---

① 张禾瑞. 近世代数基础. 北京:高等教育出版社,1978. 127. 定理 2.

② 同上. 定理 3.

对于判断整环中的元是否有真因子，该命题是很有用的，有时比用定义判断简便些．

7. 设 I 是唯一分解环，p 是 I 的素元．若 $p\,|\,a_1a_2\cdots a_n$，证明：$p\,|$ 某 a_i，$1\leqslant i\leqslant n$.

证　(用数学归纳法)$n=1$ 时，命题显然成立．

假设 n 时，命题成立．今看 $n+1$ 时，设 $p\,|\,a_1a_2\cdots a_na_{n+1}$，即 $p\,|\,(a_1a_2\cdots a_n)a_{n+1}$，则 $p\,|\,a_{n+1}$ 或 $p\,|\,a_1a_2\cdots a_n$[①]．若为前者，命题已成立；若为后者，由归纳假设，$p\,|$ 某 a_i，$1\leqslant i\leqslant n$.

所以依据归纳原理，命题得证．

8. 给出命题：$\forall\, a,b\in$ 整环 I，则 a,b 在 I 里一定有最大公因子[②]．问该命题成立吗？

答　不成立．例，$I=\{a+b\sqrt{3}\,\mathrm{i}\,|\,a,b\in\mathbb{Z}\}=\mathbb{Z}[\sqrt{3}\,\mathrm{i}]$ 是整环，但不是唯一分解环[③]．取 $\alpha=2(1+\sqrt{3}\,\mathrm{i})$，$\beta=(1+\sqrt{3}\,\mathrm{i})(1-\sqrt{3}\,\mathrm{i})=4\in I$，于是 2 和 $1+\sqrt{3}\,\mathrm{i}$ 是 α,β 的公因子，且 α,β 的所有的公因子是：单位 ±1，2 的相伴元 ±2，$1+\sqrt{3}\,\mathrm{i}$ 的相伴元 $\pm(1+\sqrt{3}\,\mathrm{i})$．在 α,β 的所有的这些公因子中，不存在公因子 δ，使任意公因子 γ，$\gamma\,|\,\delta$．比如取 $\delta=\pm1$，有公因子 2，$2\nmid\pm1$．取 $\delta=\pm2$，有公因子 $1+\sqrt{3}\,\mathrm{i}$，$1+\sqrt{3}\,\mathrm{i}\nmid\pm2$．取 $\delta=\pm(1+\sqrt{3}\,\mathrm{i})$，有公因子 2，$2\nmid\pm(1+\sqrt{3}\,\mathrm{i})$．所以 α,β 没有最大公因子．

又例，$\mathbf{R}[x^2,x^3]=\left\{\sum_{i=0}^{n}a_ix^i\in\mathbf{R}[x]\,\middle|\,n\text{ 是非负整数},a_1=0\right\}$ 是整环．由 $x\notin\mathbf{R}[x^2,x^3]$，易证 x^2,x^3 是 $\mathbf{R}[x^2,x^3]$ 的不相伴的素元．$x^6=(x^2)^3=(x^3)^2$．x^6 的分解不唯一，所以 $\mathbf{R}[x^2,x^3]$ 不是唯一分解环．取 $x^5,x^6\in\mathbf{R}[x^2,x^3]$．$x^5,x^6$ 的所有的公因子是：$\mathbf{R}$ 中的非零元，x^2,x^3 及与其相伴的元，其中并无一元可以被所有公因子整除．所以 x^2,x^3 无最大公因子．

9. 给出结论：在主理想环 I 中，如果序列 $a_1,a_2,\cdots$ 里每 a_{i+1} 都是 a_i 的真因子，$i=1,2,\cdots$，那么这个序列是有限的[④]．

1)　该结论解决了什么问题？

2)　若整环 I 不是主理想环，该结论一定不成立吗？

答　1)　该结论实质上说明了在主理想环 I 里，任一非单位的非零元 a_1 都有分解[⑤].

利用该结论可证明主理想环 $I(\neq\{0\})$ 中必存在最大理想．

事实上，设 $\mathfrak{A}_1$ 是 I 的一个理想且 $\mathfrak{A}_1\neq I$．若 $\mathfrak{A}_1$ 是最大理想，则命题已成立．若 $\mathfrak{A}_1$ 不是最大理想，又 $I\neq\{0\}$，则存在理想 $\mathfrak{A}_2$，使 $\mathfrak{A}_1\subsetneqq\mathfrak{A}_2\subsetneqq I$．若 $\mathfrak{A}_2$ 是最大理想，则命题已成立．若 $\mathfrak{A}_2$ 不是最大理想，则存在理想 $\mathfrak{A}_3$，使 $\mathfrak{A}_1\subsetneqq\mathfrak{A}_2\subsetneqq\mathfrak{A}_3\subsetneqq I$．如此继续下去，得

$$\mathfrak{A}_1\subsetneqq\mathfrak{A}_2\subsetneqq\mathfrak{A}_3\subsetneqq\cdots\subsetneqq I.$$

因 I 是主理想环，故 $\mathfrak{A}_i=(a_i)$，即 $(a_1)\subsetneqq(a_2)\subsetneqq(a_3)\subsetneqq\cdots\subsetneqq I$．于是有序列 $a_1,a_2,a_3,\cdots$ 其中 $a_{i+1}\,|\,a_i$．因 $(a_i)\neq(a_{i+1})$，故 a_{i+1} 不是 a_i 的相伴元．因 $(a_{i+1})\neq I$，故 a_{i+1} 不是单位．从而 a_{i+1} 是 a_i 的真因子，$i=1,2,\cdots$ 由该结论，这个序列一定是一个有限序列，可设 a_n 是序列里

① 张禾瑞．近世代数基础．北京：高等教育出版社，1978. 131. 定理 1.

② 同上，133. 定理 3.

③ 同上，129. 例．

④ 同上，135. 引理 1.

⑤ 同上，137. 定理的证明．

的最后一元，则$\mathfrak{A}_n=(a_n)$是最大理想．所以命题得证．

2) 未必，例，$\mathbb{Z}[\sqrt{3}\,\mathrm{i}]$不是唯一分解环，当然也不是主理想环．在$\mathbb{Z}[\sqrt{3}\,\mathrm{i}]$中，设序列$\alpha_1,\alpha_2,\cdots$里每$\alpha_{i+1}$都是$\alpha_i$的真因子，$i=1,2,\cdots$则$\exists\beta_i\in\mathbb{Z}[\sqrt{3}\,\mathrm{i}]$，使得$\alpha_i=\alpha_{i+1}\beta_i$，其中$\beta_i$也是$\alpha_i$的真因子．于是$|\alpha_i|^2=|\alpha_{i+1}|^2|\beta_i|^2$．因$\beta_i$不是单位，即$|\beta_i|^2\neq1$，故$|\beta_i|^2>1$，从而$|\alpha_i|^2>|\alpha_{i+1}|^2$，$i=1,2,\cdots$即$|\alpha_1|^2>|\alpha_2|^2>\cdots$．因$|\alpha_i|^2$是一个有限正整数，故比$|\alpha_1|^2$小的正整数只能有有限个．于是$\exists$正整数$k$，使得当$n>k$时，$\alpha_n=\alpha_k$．所以序列$\alpha_1,\alpha_2,\cdots$有限．

注 1) $\mathfrak{A}=\bigcup(a_i)$是理想的证明见第十二章，三，1，15)．

2) $\mathfrak{A}=\bigcup(a_i)=(a_n)$，其中$a_n$是序列$a_1,a_2,a_3,\cdots$里的最后一个元．

10. 试判断下面各命题是否正确．

1) 域里没有素元．

2) 不含素元的整环是零环$\{0\}$．

3) 在整环I里，设p,q都是素元且$p\mid q$，则p是q的相伴元．

4) 在整环I里，设p,q都是素元，则$pq\neq$单位．

5) 唯一分解环里任意一个元都有唯一分解．

6) 已知在整环I里$a=bc$，则a在I里有分解．

7) 在唯一分解环中，同一元的任意两个分解一定有相同的因子，只是因子的次序可能不同．

8) 唯一分解环必存在．

9) 在唯一分解环I里，

① 若$a\mid b$，则a是a,b的最大公因子．

② a是$a,0$的最大公因子．

③ $a_1,a_2,\cdots,a_n$的最大公因子是$0\Leftrightarrow a_1=a_2=\cdots=a_n=0$．

④ $a_1,a_2,\cdots,a_n$互素$\Leftrightarrow a_1,a_2,\cdots,a_n$的任一公因子都是单位．

10) 主理想环一定存在．

11) 整环是主理想环．

答 1) 正确．因域里除零元外都是单位．

2) 不正确．域就是不含素元的整环，但域不是零环．

3) 正确．事实上，因$p\mid q$，q是素元，故p只能是单位或q的相伴元．但p是素元，不是单位，从而p是q的相伴元．

4) 正确．事实上，若$pq=$单位ε，则$pq\varepsilon^{-1}=1$．于是p有逆元$q\varepsilon^{-1}\in I$，p是单位，此与p是素元矛盾．所以$pq\neq$单位．

5) 不正确．零元和单位都没有唯一分解．

6) 不正确．例，在整数环$\mathbb{Z}$里，$1=1\cdot1$，但1是$\mathbb{Z}$的单位，没有分解．

7) 不正确．在唯一分解环中，同一元的两个分解中可能因子不同，而是互为相伴元．

8) 正确．整数环$\mathbb{Z}$，数域F上一元多项式环$F[x]$，域F都是唯一分解环．

9) 正确．利用定义易证①，②，③．下面只证④．事实上，($\Rightarrow$) 因$a_1,a_2,\cdots,a_n$互素，故$a_1,a_2,\cdots,a_n$的最大公因子是单位，从而$a_1,a_2,\cdots,a_n$的任一公因子c都是单位的因子，所以c是单位(见第十四章，一，2，3))．即$a_1,a_2,\cdots,a_n$除单位外没有其他公因子．($\Leftarrow$) 因$a_1,a_2,\cdots,a_n$的任一公因子都是单位，而最大公因子首先是$a_1,a_2,\cdots,a_n$的公因子，故

$a_1,a_2,\cdots,a_n$的最大公因子也是单位．由定义，$a_1,a_2,\cdots,a_n$ 互素．

10）　正确．整数环$\mathbb{Z}$，数域 F 上一元多项式环 $F[x]$，模 n 的剩余类环 $\mathbb{Z}_n$和域都是主理想环（见第十二章，三，2 及其注 6），7））．

11）　不正确．例，$\mathbb{Z}[x]$是整环．$(2,x)$是$\mathbb{Z}[x]$的一个理想，但$(2,x)$不是$\mathbb{Z}[x]$的主理想．所以$\mathbb{Z}[x]$不是主理想环．又例，设 F 是域，则 $F[x,y]$是整环．(x,y)是 $F[x,y]$的一个理想，但不是主理想．事实上，假设$(x,y)=(f(x,y))$，又 $x,y\in(x,y)$，则 $f(x,y)\,\Big|\,x$ 且 $f(x,y)\,\Big|\,y$，即 $f(x,y)$是 x,y 的公因子．但多项式 x 和 y 的公因子只有 F 中的非零元，从而 $f(x,y)$是 $F[x,y]$的可逆元即单位，于是$(x,y)=(f(x,y))=F[x,y]$．但 $F[x,y]$中的非零元不在理想(x,y)中，产生了矛盾．因此(x,y)不是 $F[x,y]$的主理想，$F[x,y]$不是主理想环．

二、典型问题分析

1. 证明：0 不是任何元的真因子．

证　设 a 是整环 I 中任意元，而 0 是 a 的因子，则$\exists b\in I$，使得 $a=0b=0$，即 0 只能是 $a=0$的因子．但 0 是 $a=0$ 的相伴元，所以 0 不是任何元 a 的真因子．

注　1）　在整环 I 里，$0|a\Leftrightarrow a=0$.

2）　$\forall a\in$整环 I，$a\,\Big|\,0$.

由此可知零元 0 可能有真因子．例，对于整数环$\mathbb{Z}$中的 2，它既不等于 0 又不是 0 的相伴元，但 $2\,\Big|\,0$，所以 0 有真因子 2. 可是零环$\{0\}$中的零元 0 没有真因子．

2. 我们看以下的整环 I，I 刚好包含所有可以写成$\dfrac{m}{2^n}$（m 是任意整数，$n\geqslant 0$ 的整数）形式的有理数．I 的哪些元是单位，哪些元是素元？

解一　设 $m\in\mathbb{Z}$，$n\geqslant 0$ 的整数，因$\dfrac{m}{2^n}=2^{-n}m=2^iu$，其中 $i\in\mathbb{Z}$，u 是奇数，故

$$I=\left\{2^iu\,\Big|\,i\in\mathbb{Z}\ ,u\text{ 是奇数}\right\}.$$

1）　若 $\varepsilon=2^iu$ 是 I 的单位，$i\in\mathbb{Z}$，u 是奇数．则$\exists\varepsilon^{-1}\in I$，使得 $2^iu\varepsilon^{-1}=1$，其中 $1=\dfrac{1}{2^0}$是 I 的单位元．从而 $\varepsilon^{-1}=2^{-i}u^{-1}$．因 I 中元都是形如 2^iu（$i\in\mathbb{Z}$，u 为奇数）的元，故 $u=\pm1$，才能使 $\varepsilon^{-1}=2^{-i}u^{-1}\in I$. 从而 $\varepsilon=\pm2^i$，$i\in\mathbb{Z}$.

反之，设 $\varepsilon=\pm2^i$，$i\in\mathbb{Z}$，则$\exists\varepsilon^{-1}=\pm2^{-i}\in I$，使得 $\varepsilon\varepsilon^{-1}=1$，从而 ε 是 I 的单位．综上，有

$$\{I\text{ 的所有单位}\}=\left\{\pm2^i\,\Big|\,i\in\mathbb{Z}\ \right\}.$$

2）　$\{I$ 的所有素元$\}=\left\{2^iu\,\Big|\,i\in\mathbb{Z}\ ,u\text{ 是正负奇素数}\right\}$.

事实上，$\forall 2^iu\in\{I$ 的所有素元$\}$，$i\in\mathbb{Z}$，u 是奇数．因 2^i 是单位，故 u 是 I 的素元．下面证明 u 是$\mathbb{Z}$的素数．假设不然，u 不是$\mathbb{Z}$的素数，又 $u\neq0$，$u\neq I$ 的单位$\pm2^i$，$i\in\mathbb{Z}$，从而 u 在$\mathbb{Z}$中有真因子 u_1，使得 $u=u_1u_2$. 由第十四章，一，6，u_2 也是 u 在$\mathbb{Z}$中的真因子．即 $u_i\neq$ $\mathbb{Z}$的单位±1. 又因 u 是奇数，故 u_i 是奇数，即 $u_i\neq I$ 的单位，$i=1,2$. 由第十四章，一，6，u 在 I 中有真因子．因此 u 不是 I 的素元，发生了矛盾．从而 u 是$\mathbb{Z}$的素数．于是

$$\{I\text{ 的所有素元}\}\subset\left\{2^iu \,\middle|\, i\in\mathbb{Z},u\text{ 是正负奇素数}\right\}.$$

反之，$\forall\, 2^iu\in\left\{2^iu \,\middle|\, i\in\mathbb{Z},u\text{ 是正负奇素数}\right\}$，$i\in\mathbb{Z}$，$u$ 是奇素数．要证 2^iu 是 I 的素元，因 2^i 是单位，故只需证 u 是 I 的素元．设 $2^{i_1}u_1(\in I)$是 u 的任一因子，则

$$u=(2^{i_1}u_1)(2^{i_2}u_2)=2^{i_1+i_2}u_1u_2,$$

其中 $2^{i_2}u_2\in I$. 因 u,u_1,u_2 都是奇数，故 $i_1+i_2=0$，从而 $u=u_1u_2$. 因 u 是素数，故 u_1 是 u 在 $\mathbb{Z}$ 中的平凡因子，只能 $u_1=\mathbb{Z}$ 的单位 ±1 或 $u_1=u$ 的相伴元 $\pm u$. 若 $u_1=\pm1$，则 $2^{i_1}u_1=\pm2^{i_1}$ 是 I 的单位；若 $u_1=\pm u$，则 $2^{i_1}u_1=\pm2^{i_1}u$ 是 u 的相伴元．即 u 在 I 里只有平凡因子．又 $u\neq0$，$u\neq I$ 的单位，因而 u 是 I 的素元．而且 2^iu 也是 I 的素元．于是

$$\left\{2^iu \,\middle|\, i\in\mathbb{Z},u\text{ 是正负奇素数}\right\}\subset\{I\text{ 的所有素元}\}.$$

所以

$$\{I\text{ 的所有素元}\}=\left\{2^iu \,\middle|\, i\in\mathbb{Z},u\text{ 是正负奇素数}\right\}.$$

解二

1) $\frac{m}{2^n}(\in I)$是单位 $\Leftrightarrow m=\pm2^k$，$k\geqslant0$ 的整数．

事实上，($\Rightarrow$) 因$\frac{m}{2^n}$是 I 的单位，故 $\exists\,\frac{m_1}{2^{n_1}}\in I$，使得$\frac{m}{2^n}\cdot\frac{m_1}{2^{n_1}}=1$，即 $mm_1=2^{n+n_1}$，从而在 $\mathbb{Z}$ 中，$m\mid 2^{n+n_1}$. 因 2 是 $\mathbb{Z}$ 的素数，$n+n_1$ 是大于或零于 0 的整数，故 $m=\pm2^k$，$k\geqslant0$ 的整数．

($\Leftarrow$) 因 $m=\pm2^k$，$k\geqslant0$ 的整数，即$\frac{m}{2^n}=\pm\frac{2^k}{2^n}$，故 $\exists\pm\frac{2^n}{2^k}\in I$，使得$\left(\pm\frac{2^k}{2^n}\right)\left(\pm\frac{2^n}{2^k}\right)=1$，从而$\frac{m}{2^n}$有逆元$\pm\frac{2^n}{2^k}\in I$. 所以$\frac{m}{2^n}$是单位．

2) $\frac{m}{2^n}(\in I)$是素元 $\Leftrightarrow m=\pm2^kp$，$p$ 是正奇素数，$k\geqslant0$ 的整数．

事实上，($\Rightarrow$) 因$\frac{m}{2^n}(\in I)$是素元，故$\frac{m}{2^n}\neq0$，$\frac{m}{2^n}\neq I$ 的单位，即 $m\neq0$，$m\neq\pm2^k$，$k\geqslant0$ 的整数．因为对于整数 m 来说，有 $m=\pm2^kp$，$k\geqslant0$ 的整数，$p=0$ 或 p 是正奇数，所以 $p\neq0$，$p\neq1$. 下面证明 p 是素数．假设 p 不是素数，又 $p\neq1$，即 p 是合数，从而 $p=p_1p_2$，$1<p_i<p$. 因 p 是奇数，故 p_i 是奇数，$i=1,2$. 于是

$$\frac{m}{2^n}=\frac{\pm2^kp_1}{2^n}\cdot\frac{p_2}{2^0},$$

其中$\frac{\pm2^kp_1}{2^n}\neq$单位，$\frac{p_2}{2^0}\neq$单位．又$\frac{m}{2^n}\neq0$，由第十四章，一，6，$\frac{m}{2^n}$在 I 中有真因子，此与$\frac{m}{2^n}$是素元矛盾．因而 p 是素数．所以必要性得证．

($\Leftarrow$) 已知 $m=\pm2^kp$，p 是正奇素数，$k\geqslant0$ 的整数，从而$\frac{m}{2^n}=\frac{\pm2^kp}{2^n}\neq0$ 且$\neq$单位．设$\frac{m_1}{2^{n_1}}$是$\frac{\pm2^kp}{2^n}$的因子，则

$$\frac{\pm2^kp}{2^n}=\frac{m_1}{2^{n_1}}\cdot\frac{m_2}{2^{n_2}},$$

其中$\frac{m_2}{2^{n_2}}\in I$. 于是$\pm 2^{k+n_1+n_2}p=2^n m_1 m_2$，从而在$\mathbb{Z}$中，$m_1\mid\pm 2^{k+n_1+n_2}p$. 因2与$p$都是素数，$k+n_1+n_2$是大于或等于0的整数，故$m_1=\pm 2^{k_1}$或$\pm 2^{k_1}p$，其中$k_1$是大于或等于0的整数．若$m_1=\pm 2^{k_1}$，则$\frac{m_1}{2^{n_1}}=$单位．若$m_1=\pm 2^{k_1}p$，则$\frac{m_1}{2^{n_1}}=\frac{\pm 2^{k_1}p}{2^{n_1}}=\frac{2^{k_1}2^n}{2^k 2^{n_1}}\left(\frac{\pm 2^k p}{2^n}\right)=\frac{2^{k_1+n}}{2^{k+n_1}}\cdot\frac{m}{2^n}$，其中$\frac{2^{k_1+n}}{2^{k+n_1}}$是单位．因此，$\frac{m_1}{2^{n_1}}$是$\frac{m}{2^n}$的相伴元．于是$\frac{m}{2^n}$只有平凡因子．所以$\frac{m}{2^n}$是素元．

解三　下面再给出证明

$$\frac{m}{2^n}(\in I)\text{是素元}\Rightarrow m=\pm 2^k p,\ p\text{是正奇素数},k\geqslant 0\text{的整数的一个方法}.$$

设$\frac{m}{2^n}$是I的素元．对于整数m来说，总有

$$m=\pm 2^k p,k\geqslant 0\text{的整数},\ p=0\text{或}p\text{是正奇数}.$$

下面只需证明p是素数．因$\frac{m}{2^n}$是素元，故$m\neq 0,m\neq\pm 2^k$，从而$p\neq 0,p\neq 1$. 可将p在$\mathbb{Z}$里进行分解：$p=p_1p_2\cdots p_r$，其中p_i是素数，因p是奇数，故p_i也是奇数，$i=1,2,\cdots,r$.

若$r=1$，则$p=p_1$是素数，命题已证．

若$r>1$，则

$$\frac{m}{2^n}=\frac{\pm 2^k p}{2^n}=\frac{\pm 2^k p_1}{2^n}\cdot\frac{p_2p_3\cdots p_r}{2^0},$$

其中$\frac{\pm 2^k p_1}{2^n}\neq$单位，$\frac{p_2p_3\cdots p_r}{2^0}\neq$单位．又$\frac{m}{2^n}\neq 0$，从而由第十四章，一，6，$\frac{m}{2^n}$有真因子，此与$\frac{m}{2^n}$是素元矛盾．所以$r$不能大于1，只能$r=1$. 于是命题得证．

注　1)　由第九章，四，1，7)知I是一个环，又I是含单位元$1=\frac{1}{2^0}$的数环，从而易知I是整环．

2)　由解一知：设u是奇数，则

$$u\text{是}I\text{的素元}\Leftrightarrow u\text{是}\mathbb{Z}\text{的奇素数}.$$

3)　因$7=\frac{1}{2}\cdot 14=2^{-1}\cdot 14$，其中$2^{-1}\in I$，故在$I$里，$14\mid 7$. 在$\mathbb{Z}$里，显然$14\nmid 7$. 因此，若$S$是整环$R$的子整环，那么，如果$a,b\in S$，在$R$里有$a\mid b$，而在$S$里却未必有$a\mid b$. 但在$S$里有$a\mid b$，则必在$R$里也有$a\mid b$.

4)　2是I的单位，但2不是$\mathbb{Z}$的单位．说明了整环R的单位未必是子整环S的单位．但$S(\neq\{0\})$的单位必为R的单位．

5)　2是$\mathbb{Z}$的素元，但2不是I的素元，而是I的单位．这说明了：若S是整环R的子整环，则子整环S的素元未必是整环R的素元．

例，3是$\mathbb{Z}$的素元，但3不是$\mathbb{Q}$的素元．又例，7是$\mathbb{Z}$的素元，但7在整环$\mathbb{Z}[\sqrt{3}\,\mathrm{i}]=\{a+b\sqrt{3}\,\mathrm{i}\mid a,b\in\mathbb{Z}\}$中可写成：$7=(2+\sqrt{3}\,\mathrm{i})(2-\sqrt{3}\,\mathrm{i})$，其中$2\pm\sqrt{3}\,\mathrm{i}$都不是$I$的单位，从而7有真因子，7不是$\mathbb{Z}[\sqrt{3}\,\mathrm{i}]$的素元．又例，$x^2-2$是$\mathbb{Q}[x]$的素元，但$x^2-2$不是$\mathbb{R}[x]$的素元．

6)　$6=2\cdot 3$是I的素元，但6不是$\mathbb{Z}$的素元．即整环R的素元p未必是子整环S的

素元．即使 $p\in S$，p 也未必是 S 的素元．

3. I 是刚好包含所有复数 $a+bi$（a,b 是整数）的整环．证明：5 不是 I 的素元．5 有没有唯一分解？

证 1） ε 是 I 的单位 $\Leftrightarrow |\varepsilon|^2=1 \Leftrightarrow \varepsilon=\pm 1,\varepsilon=\pm i$.

事实上，($\Rightarrow$) 设 $\varepsilon=a+bi$ 是 I 的单位，则 $\exists\, \varepsilon^{-1}\in I$，使得 $\varepsilon\varepsilon^{-1}=1$，从而 $|\varepsilon\varepsilon^{-1}|^2=|1|^2$，即 $|\varepsilon|^2|\varepsilon^{-1}|^2=1$. 因 $\varepsilon\neq 0$，故 $|\varepsilon|^2=a^2+b^2$ 是正整数，同样 $|\varepsilon^{-1}|^2$ 也是正整数．因此，$|\varepsilon|^2=1$. 即 $a^2+b^2=1$，于是 $a=\pm 1,b=0$ 或 $a=0,b=\pm 1$. 所以 $\varepsilon=a+bi$ 是 ± 1 或 $\pm i$.

($\Leftarrow$) 设 $\varepsilon=a+bi\in I$，$|\varepsilon|^2=1$，则 $a^2+b^2=1$，从而 $a=\pm 1,b=0$ 或 $a=0,b=\pm 1$，即 $\varepsilon=\pm 1$ 或 $\pm i$. 因 ± 1 有逆元 ± 1，$\pm i$ 有逆元 $\mp i$，故 ± 1，$\pm i$ 都是 I 的单位，即 ε 是 I 的单位．

2） $\alpha\in I$，$|\alpha|^2=5\Rightarrow \alpha$ 是素元．

事实上，因 $|\alpha|^2=5$，故 $\alpha\neq 0$. 因 $|\alpha|^2\neq 1$，故由 1）知 α 不是单位．设 β 是 α 在 I 中的任一因子，则 $\exists\,\gamma\in I$，使得 $\alpha=\beta\gamma$. 从而

$$5=|\alpha|^2=|\beta\gamma|^2=|\beta|^2|\gamma|^2.$$

因 $|\beta|^2$，$|\gamma|^2$ 都是正整数，故 $|\beta|^2$ 只能是 1 或 5. 若 $|\beta|^2=1$，则 β 是单位；若 $|\beta|^2=5$，则 $|\gamma|^2=1$，即 γ 是单位，从而 $\beta=\alpha\gamma^{-1}$，其中 γ^{-1} 是单位．于是 β 是 α 的相伴元．因此 α 只有平凡因子．所以 α 是素元．

3） 5 不是 I 的素元．

事实上，因 $5=(1+2i)(1-2i)$，其中 $1\pm 2i$ 不是单位，$5\neq 0$. 由第十四章，一，6，5 有真因子，故 5 不是 I 的素元．

4） 假设 $5=p_1p_2\cdots p_n$，其中 p_i 是素元，$i=1,2,\cdots,n$. 因 5 不是素元，故 $n\neq 1$. 又因 $25=|5|^2=|p_1|^2|p_2|^2\cdots|p_n|^2$. 因 p_i 不是单位，故 $|p_i|^2\neq 1$，又 $|p_i|^2\neq 2,3,4$，从而 $|p_i|^2=5$. 所以只能 $n=2$.

设 $5=\alpha\beta$，其中 $\alpha=a+bi,\beta\in I$. 则 $25=|5|^2=|\alpha|^2|\beta|^2$. 因 $|\alpha|^2$，$|\beta|^2$ 都是正整数，故 $|\alpha|^2$ 只可能是 1 或 5 或 25. 若 $|\alpha|^2=1$，则 α 是单位；若 $|\alpha|^2=25$，则 $|\beta|^2=1$，即 β 是单位，从而只能考虑 $|\alpha|^2=5$，即 $a^2+b^2=5$，只能 $a=\pm 1,b=\pm 2$ 或 $a=\pm 2,b=\pm 1$. 因此，

$$5=(1+2i)(1-2i)=(-1-2i)(-1+2i)=(2+i)(2-i)=(-2-i)(-2+i).$$

因 $|1\pm 2i|^2=|-1\pm 2i|^2=|2\pm i|^2=|-2\pm i|^2=5$，故由 2），$1\pm 2i$，$-1\pm 2i$，$2\pm i$，$-2\pm i$ 都是素元．上面 4 个式子就是 5 的一切可能的素元分解．因 $-1-2i=(-1)(1+2i)$，$2-i=(-i)(1+2i)$，$-2+i=i(1+2i)$，$-1+2i=(-1)(1-2i)$，$2+i=i(1-2i)$，$-2-i=(-i)(1-2i)$. 故 $-1-2i$，$2-i$，$-2+i$ 都是 $1+2i$ 的相伴元，$-1+2i$，$2+i$，$-2-i$ 都是 $1-2i$ 的相伴元．所以 5 有唯一分解．

注 1） 设 $|\alpha|^2=$ 素数 p，则 α 是 I 的素元．

此命题仿 2）的证明方法可证．

2） 注 1）中命题只是 I 的素元的充分条件，而不是必要条件．例，$|3|^2=9$ 不是素数，但 3 是 I 的素元．这是因为，$3\neq 0$，$3\neq$ 单位．若 $\alpha=a+bi(\in I)$ 是 3 的因子，则 $\exists\,\beta\in I$，使得 $3=\alpha\beta$. 从而 $9=|3|^2=|\alpha|^2|\beta|^2$，于是 $|\alpha|^2$ 只可能是 1 或 3 或 9. 但 $|\alpha|^2\neq 3$（因 $a^2+b^2\neq 3$），因此 $|\alpha|^2=1$ 或 9. $|\alpha|^2=1$ 时，α 是单位；$|\alpha|^2=9$ 时，$|\beta|^2=1$，即 β 是单位，那么 α 是 3 的相伴元．所以 3 只有平凡因子，3 是素元．

实际上，设 $|\alpha|^2=9$，则 α 是素元．

3)　下面给出 $I=\{a+bi \mid a,b\in\mathbb{Z}\}=\mathbb{Z}[i]$的素元的充分必要条件．设 $\alpha=a+bi\in I$,

①　若 $ab\neq 0$,则

$$|\alpha|^2 \text{ 是 } \mathbb{Z} \text{ 的素数} \Leftrightarrow \alpha \text{ 是 } I \text{ 的素元}.$$

②　若 $ab=0$,则

$$|\alpha| \text{ 是 } \mathbb{Z} \text{ 的素数且 } 4 \mid |\alpha|-3 \Leftrightarrow \alpha \text{ 是 } I \text{ 的素元}.$$

证明略．由该命题知,若 $a\in\mathbb{Z}$,而 a 不是 $\mathbb{Z}$ 的素数,则 a 一定不是 I 的素元．例,6 不是素数,则 6 不是 I 的素元,实际上,6 有真因子 2i. 但若 $a\in\mathbb{Z}$,即使 a 是 $\mathbb{Z}$ 的素数,a 也未必是 I 的素元．例,2 是素数,但 $4\nmid 2-3$,从而 2 不是 I 的素元,实际上,$1+i$ 是 2 的真因子. 13 是素数,但 $4\nmid 13-3$,从而 13 不是 I 的素元,实际上,13 有真因子 $2+3i$. 17 是素数,但 $4\nmid 17-3$,从而 17 不是 I 的素元,实际上,17 有真因子 $1+4i$. 由本题已知 5 是素数,但 5 不是 I 的素元．又如 7 是 $\mathbb{Z}$ 的素数,且 $4\mid 7-3$,从而 7 是 I 的素元,仿本题证明中的 2)也可直接证明.

$7-i$ 不是 I 的素元,因为 $|7-i|^2=50$ 不是 $\mathbb{Z}$ 的素数,实际上,$7-i=(2-i)^2(1+i)$,其中 $2-i,1+i$ 都是 I 的素元．

4. 证明:设 I 是唯一分解环,

1)　$\forall a_1,a_2,\cdots,a_n\in I$, $a_1,a_2,\cdots,a_n$ 有最大公因子 $\in I$.

2)　d,d' 是 $a_1,a_2,\cdots,a_n$ 的两个最大公因子 $\Rightarrow d'=\varepsilon d$, ε 是单位．

证　1)　用数学归纳法．

当 $n=2$ 时,(略).

假定对于 $n-1$ 个元来说命题成立．今看 n 个元 $a_1,a_2,\cdots,a_n$ 时．由归纳假定,可设 d_1 是 $a_1,a_2,\cdots,a_{n-1}$ 的一个最大公因子．再设 d 是 d_1,a_n 的一个最大公因子,则 d 就是 $a_1,a_2,\cdots,a_n$ 的一个最大公因子．事实上,$d\mid a_n$, $d\mid d_1$,又 $d_1\mid a_i$, $i=1,2,\cdots,n-1$. 从而 $d\mid a_j$, $j=1,2,\cdots,n-1,n$,即 d 是 $a_1,a_2,\cdots,a_n$ 的一个公因子．假定 c 是 $a_1,a_2,\cdots,a_n$ 的任一公因子,当然 $c\mid a_i$, $i=1,2,\cdots,n-1$,从而 $c\mid d_1$,又 $c\mid a_n$,于是 $c\mid d$. 所以 d 是 $a_1,a_2,\cdots,a_n$ 的一个最大公因子．

由归纳原理,命题得证．

2)　若 d,d' 都是 $a_1,a_2,\cdots,a_n$ 的最大公因子,则 $d'\mid d$, $d\mid d'$,从而由第十四章,一,3,1),$d'=\varepsilon d$, ε 是单位．

注　由该命题知:在唯一分解环里,若 d 是 $a_1,a_2,\cdots,a_n$ 的一个最大公因子,则

$$d' \text{ 是 } a_1,a_2,\cdots,a_n \text{ 的一个最大公因子} \Leftrightarrow d'=\varepsilon d,\ \varepsilon \text{ 是单位}.$$

即,若 d 是 $a_1,a_2,\cdots,a_n$ 的一个最大公因子,则 $a_1,a_2,\cdots,a_n$ 的全部最大公因子就是 d 的全部相伴元．

5. 假定在一个唯一分解环里,$a_1=db_1$, $a_2=db_2$, $\cdots$, $a_n=db_n$. 证明:当而且只当 d 是 $a_1,a_2,\cdots,a_n$ 的一个最大公因子的时候,$b_1,b_2,\cdots,b_n$ 互素．这里 $d\neq 0$.

证　($\Rightarrow$)　已知 d 是 $a_1,a_2,\cdots,a_n$ 的一个最大公因子．设 d' 是 $b_1,b_2,\cdots,b_n$ 的任一公因子,则有 $b_i=d'c_i$, $i=1,2,\cdots,n$. 从而 $a_i=dd'c_i$,即 dd' 是 $a_1,a_2,\cdots,a_n$ 的公因子,于是 $dd'\mid d$. 又 $d\mid dd'$,因此 $dd'=d\varepsilon$, ε=单位．由 $d\neq 0$ 及消去律,$d'=\varepsilon$ 是单位,所以 $b_1,b_2,\cdots$,

b_n 互素(见第十四章,一,10,9),④).

($\Leftarrow$) 已知 $b_1,b_2,\cdots,b_n$ 互素. 设 d' 是 $a_1,a_2,\cdots,a_n$ 的一个最大公因子,则 $d \mid d'$,从而 $d'=ds$. 下面证明 s 是单位. 因 d' 是 $a_1,a_2,\cdots,a_n$ 的一个公因子,故 $a_i=d'c_i=dsc_i=db_i$. 由 $d\neq 0$ 及消去律,$sc_i=b_i$,$i=1,2,\cdots,n$,即 S 是 $b_1,b_2,\cdots,b_n$ 的公因子. 因 $b_1,b_2,\cdots,b_n$ 互素,故 S 是单位. 从而由 $d'=ds$ 有 $d=d's^{-1}$,其中 s^{-1} 是单位,所以 d 是 $a_1,a_2,\cdots,a_n$ 的最大公因子.

6. 假定 I 是一个整环,(a) 和 (b) 是 I 的两个主理想. 证明:$(a)=(b)$ 当且只当 b 是 a 的相伴元的时候.

证 ($\Rightarrow$) 设 $(a)=(b)$,则 $a\in(b)$,$b\in(a)$. 因 I 是有单位元的交换环,故 $\exists c,c'\in I$,使得 $a=cb$,$b=c'a$,即 $b \mid a$,$a \mid b$. 所以 b 是 a 的相伴元(见第十四章,一,3,1)).

($\Leftarrow$) 设 $b=\varepsilon a$,ε 是单位,则 $a=\varepsilon^{-1}b$. 从而 $b\in(a)$,$a\in(b)$. 于是 $(b)\subset(a)$,$(a)\subset(b)$. 所以 $(a)=(b)$.

注 由该命题容易得出下面结论:在整环 I 里,

1) $a \mid b \Leftrightarrow (a)\supset(b)$.

注意,因子 a 对应着"较大"的主理想 (a)(参看第六章,三,5).

2) a 是 b 的真因子 $\Rightarrow (a)\supsetneqq(b)$.

该命题的逆命题不成立. 例,$\mathbb{Z}=(1)\supsetneqq(2)=2\mathbb{Z}$,但 1 只是 2 的因子而不是真因子.

3) a 是 b 的真因子 $\Leftrightarrow (a)\supsetneqq(b)$ 且 a 不是单位.

事实上,($\Rightarrow$) 显然. ($\Leftarrow$) 由 $(a)\supset(b)$,$a \mid b$. 已知 $a\neq$ 单位,且 $a\neq b$ 的相伴元. 不然,若 $a=b$ 的相伴元,则 $(a)=(b)$,此与已知矛盾. 所以 a 是 b 的真因子.

4) ε 是单位 $\Leftrightarrow \varepsilon$ 是 1 的相伴元 $\Leftrightarrow (\varepsilon)=(1)=I$(见第十四章,一,4,2)和第九章,一,4,9)).

5) 主理想的生成元未必只有一个. 例,高斯整数环 $\mathbb{Z}[\mathrm{i}]$ 有且只有 4 个单位 $\pm 1,\pm\mathrm{i}$. 从而 $a+b\mathrm{i}$ 的相伴元有且只有 $a+b\mathrm{i},-a-b\mathrm{i},b-a\mathrm{i},-b+a\mathrm{i}$. 所以 $\mathbb{Z}[\mathrm{i}]$ 的主理想 $(a+b\mathrm{i})=(-a-b\mathrm{i})=(b-a\mathrm{i})=(-b+a\mathrm{i})$.

7. 假定 I 是一个主理想环,并且 $(a,b)=(d)$. 证明:d 是 a 和 b 的一个最大公因子,因此 a 和 b 的任何最大公因子 d' 都可以写成以下形式:$d'=sa+tb(s,t\in I)$.

证一 1) 因 I 是主理想环,故 a,b 生成的理想 (a,b) 是一个主理想,设为 (d),则 $a,b\in(a,b)=(d)$,从而 $d \mid a$,$d \mid b$. 设 c 是 a,b 的任一公因子,则 $c \mid a$,$c \mid b$. 又 $d\in(d)=(a,b)$,因此,$\exists s',t'\in I$,使得 $d=s'a+t'b$. 于是 $c \mid s'a+t'b=d$. 所以 d 是 a,b 的一个最大公因子.

2) 设 d' 是 a,b 的任一最大公因子. 由 1)知 $(a,b)=(d)$ 中的 $d=s'a+t'b(s',t'\in I)$ 是 a,b 的一个最大公因子,从而 $d'=\varepsilon d=\varepsilon(s'a+t'b)=(\varepsilon s')a+(\varepsilon t')b=sa+tb$,其中 $s=\varepsilon s'$,$t=\varepsilon t'\in I$,ε 是 I 的单位.

证二 1) 同上法证明 d 是 a,b 的一个公因子. 若 c 是 a,b 的任一公因子,则 $c \mid a$,$c \mid b$. 从而 $a\in(c)$,$b\in(c)$,因此 $(a,b)\subset(c)$. 由 $d\in(d)=(a,b)\subset(c)$,有 $c \mid d$. 所以 d 是 a,b 的一个最大公因子.

2）设 d' 是 a,b 的任一最大公因子．则 $d'=\varepsilon d$，ε 是单位．由第十四章，二，6，$(d')=(d)=(a,b)$，从而 $d'\in(a,b)$，于是，$\exists\, s,t\in I$，使得 $d'=sa+tb$.

注　1）在主理想环 I 里，

① $(a,b)=(d)\Leftrightarrow d$ 是 a,b 的一个最大公因子．

② d' 是 a,b 的一个最大公因子 $\Leftrightarrow d'$ 是 a,b 的一个公因子，且 $\exists\, s,t\in I$，使得 $d'=sa+tb$.

事实上，①（$\Rightarrow$）由本命题已知．（$\Leftarrow$）因 I 是主理想环，故可设理想 $(a,b)=(d_1)$，则由本命题知，d_1 是 a,b 的一个最大公因子．且 $d=\varepsilon d_1$，ε 是单位．由第十四章，二，6，$(d)=(d_1)=(a,b)$.

②（$\Rightarrow$）由本命题已知．（$\Leftarrow$）已知 d' 是 a,b 的一个公因子．设 c 是 a,b 的任一公因子，则 $c\,|\,sa+tb=d'$. 所以 d' 是 a,b 的一个最大公因子．

2）可推广为下面命题：设 I 是主理想环，则

① $(a_1,a_2,\cdots,a_n)=(d)\Leftrightarrow d$ 是 $a_1,a_2,\cdots,a_n$ 的一个最大公因子．

② d' 是 $a_1,a_2,\cdots,a_n$ 的一个最大公因子 $\Leftrightarrow d'$ 是 $a_1,a_2,\cdots,a_n$ 的一个公因子，且 $\exists\, s_i\in I$，$i=1,2,\cdots,n$，

使得 $d'=s_1a_1+s_2a_2+\cdots+s_na_n$.

3）本命题说明，主理想环中任意元 $a_1,a_2,\cdots,a_n$ 都有最大公因子．当然由 I 是主理想环，从而是唯一分解环，也可说明在 I 中最大公因子的存在性．

4）例，在主理想环 $\mathbb{Q}[x]$ 中，因 $x+1$ 是 $x^2-1,(x+1)^2$ 的一个最大公因子，$x+1$ 也是 $3x^2+x-2,x^3+x^2-x-1$ 的一个最大公因子，故 $(x^2-1,(x+1)^2)=x+1$，$(3x^2+x-2,x^3+x^2-x-1)=x+1$.

5）设 I 不是主理想环而是整环，那么虽 d 是 a,b 的一个最大公因子，却未必 $\exists\, s,t\in I$，使得 $d=sa+tb$. 例，$\mathbb{Z}[x]$ 不是主理想环（第十二章，二，3，注 2））. 虽 1 是 $2,x$ 的一个最大公因子，但 $\bar{\exists}\, u(x),v(x)\in\mathbb{Z}[x]$，使得 $1=2u(x)+xv(x)$. 又例，设 F 是域，则 $F[x,y]$ 是整环，但不是主理想环（第十四章，一，10，11））. 虽 x,y 互素，但 $\forall\, u(x,y),v(x,y)\in F[x,y]$，都使 $xu(x,y)+yv(x,y)\neq 1$.

6）在主理想环里，若 d 是 a,b 的最大公因子，则 $(a)\subset(d)$，$(b)\subset(d)$，$(a)\cap(b)\subset(d)$，$(a)\cup(b)\subset(d)$.

7）参看第十二章，二，4，注 4），5）与第十二章，三，2，注 5）.

8. 一个主理想环的非零最大理想都是由一个素元所生成的．

证一　设 (p) 是主理想环 I 的一个非零最大理想，则 $p\neq 0$. 因 $(p)\neq I$，故 $p\neq$ 单位．若 p 不是素元，则 p 有真因子 $b\in I$. 由第十四章，二，6，注 3），4），$I\supsetneqq(b)\supsetneqq(p)$，此与 (p) 是最大理想矛盾．所以 p 是素元．

证二　设 (p) 是主理想环 I 的一个非零最大理想，则 $p\neq 0$，$p\neq$ 单位．因 I 是唯一分解环，故 p 有分解，$\exists$ 素元 $q\in I$，使得 $q\,|\,p$. 显然 $q\neq$ 单位．从而 $I\supsetneqq(q)\supset(p)$. 因 (p) 是最大理想，故 $(q)=(p)$. 由第十四章，二，6，p 是素元 q 的相伴元．所以 p 是素元．

证三　设 (p) 是主理想环 I 的一个非零最大理想，则 $p\neq 0$，$p\neq$ 单位．若 p 不是素元，则 p 有真因子 $b\in I$，使得 $p=bc$，且 c 也是 p 的真因子，从而 $p\nmid b$，$p\nmid c$. 于是在 I 的模 (p) 的剩余类环 $I/(p)$ 中，$[b]\neq[0]$，$[c]\neq[0]$. 但 $[p]=[bc]=[b][c]=[0]$，即 $I/[p]$ 有零因子．

因此 $I/(p)$ 不是域(实际上，$I/(p)$ 连整环也不是)．而 I 是有单位元的交换环，由第十三章，一，4 知 (p) 不是最大理想，矛盾．所以 p 是素元．

注 1) 由证三知：在主理想环 I 里，若 p 不是素元，且 $p\neq 0$，$p\neq$ 单位，则 $I/(p)$ 不是整环.

2) 由本命题知：设 I 是主理想环，$p(\neq 0)\in I$，则

$$p \text{ 是 } I \text{ 的素元} \Leftrightarrow (p) \text{ 是 } I \text{ 的最大理想}^{①}.$$

3) 由本命题及第十三章，一，4 知：设 I 是主理想环，$p(\neq 0)\in I$，则

$$p \text{ 是 } I \text{ 的素元} \Leftrightarrow I/(p) \text{ 是域}.$$

例 $\mathbb{Z}[i]$ 是主理想环，$3(\neq 0)\in\mathbb{Z}[i]$．由第十四章，二，3，注 2)，3 是 $\mathbb{Z}[i]$ 的素元，从而 (3) 是 $\mathbb{Z}[i]$ 的最大理想，$\mathbb{Z}[i]/(3)$ 是域．

4) 本命题是第十三章，一，2 的推广．

5) 设 I 是整环，$p\in I$，则

$$\text{若 } p\mid ab \text{，有 } p\mid a \text{ 或 } p\mid b \Leftrightarrow I/(p) \text{ 是整环}.$$

事实上，$(\Rightarrow)$ 因 I 是整环，故 $I/(p)$ 是一个含单位元 $1+(p)$ 的交换环．下面只需证 $I/(p)$ 无零因子．设 $[a],[b]\in I/(p)$．若 $[a][b]=[ab]=[0]$，则 $p\mid ab$，由已知，$p\mid a$ 或 $p\mid b$. 从而 $[a]=[0]$ 或 $[b]=[0]$．因此 $I/(p)$ 无零因子．所以 $I/(p)$ 是整环．

$(\Leftarrow)$ 若 $p\mid ab$，则 $[ab]=[a][b]=[0]$．因 $I/(p)$ 是整环，无零因子，故 $[a]=[0]$ 或 $[b]=[0]$，从而 $p\mid a$ 或 $p\mid b$.

9. 我们看两个主理想环 I 和 I_0，I_0 是 I 的子环．假定 a 和 b 是 I_0 的两个元，d 是这两个元在 I_0 里的一个最大公因子．证明：d 也是这两个元在 I 里的一个最大公因子．

证 因 d 是 a,b 在 I_0 里的一个公因子，故 $\exists\, a',b'\in I_0\subset I$，使得 $a=a'd$，$b=b'd$．从而 d 是 a,b 在 I 里的一个公因子．

设 c 是 a,b 在 I 里的任一公因子，则 $\exists\, a_1,b_1\in I$，使得 $a=a_1c$，$b=b_1c$．因 d 是 a,b 在主理想环 I_0 里的一个最大公因子，故由第十四章，二，7，$\exists\, s,t\in I_0$，使得 $d=sa+tb$．当然此式在 I 里仍成立．从而

$$d=s(a_1c)+t(b_1c)=(sa_1+tb_1)c,$$

其中 $sa_1+tb_1\in I$．于是在 I 里，$c\mid d$.

所以 d 是 a,b 在 I 里的一个最大公因子．

注 1) 由证明可见：将本命题中的 I 减弱为整环，结论仍成立．

2) 本命题的逆命题不成立，即：设 I,I_0 都是主理想环，I_0 是 I 的子环，$a,b\in I_0$，d 是 a,b 在 I 里的一个最大公因子，但 d 却未必是 a,b 在 I_0 里的一个最大公因子．

例 $\mathbb{Q}$，$\mathbb{Z}$ 都是主理想环，$\mathbb{Z}$ 是 $\mathbb{Q}$ 的子环，$1,3\in\mathbb{Z}$，4 是 1，3 在 $\mathbb{Q}$ 里的一个最大公因子，但 4 不是 1，3 在 $\mathbb{Z}$ 里的一个最大公因子．实际上，1，3 在 $\mathbb{Q}$ 里的最大公因子是任一非零有理数，1，3 在 $\mathbb{Z}$ 里的最大公因子只能是 ± 1.

---

① 张禾瑞．近世代数基础．北京：高等教育出版社．1978. 136. 引理 2.

三、讲与练

1. 判断下列各命题是否正确．

1)　设 $a,b\in$ 整环 I，$a\mid b$，则 $(a,b)=(a)$．

2)　p 是 $\mathbb{Z}$ 的正或负素数 $\Leftrightarrow$ p 是 $\mathbb{Z}$ 的素元．

3)　$[2]$是 $\mathbb{Z}_5$ 的素元．

4)　-17 是 $\mathbb{Z}$ 的素元．

5)　$\mathbb{Z}$ 的理想$(21,56,147)=(7)$．

6)　无限理想列$(2)\subset(4)\subset(8)\subset\cdots$的存在，表示 $\mathbb{Z}$ 不是一个主理想环．

7)　$\mathbb{Z}$ 的理想$(2,4,8,16)$不是主理想．

8)　主理想环的子整环是主理想环．

9)　若整环 I 的子整环是主理想环，则 I 也是主理想环．

10)　设ϕ是整环 I 到整环 $\bar{I}$ 的一个同态满射．

①　若 $b\mid a$，则$\phi(b)\mid\phi(a)$．

②　若 a,b 相伴，则$\phi(a)$，$\phi(b)$相伴．

③　若 p 是 I 的素元，则$\phi(p)$也是 $\bar{I}$ 的素元．

④　若 U 是由 I 的所有单位作成的乘群，$\overline{U}$是由 $\bar{I}$ 的所有单位作成的乘群，则ϕ是群 U 到群 $\overline{U}$ 的一个同态满射．

解　1)　正确．事实上，因 $a\mid b$，故 $b\in(a)$，又 $a\in(a)$，从而$(a,b)\subset(a)$；显然$(a)\subset(a,b)$．所以$(a,b)=(a)$．

2)　正确．依定义直接可知．

3)　不正确．因$[2]$是 $\mathbb{Z}_5$ 的单位．

4)　正确．

5)　正确．因 $\mathbb{Z}$ 是主理想环，7 是 21，56，147 的一个最大公因子，故由第十四章，二，7，注 2)知，$(21,56,147)=(7)$．

6)　不正确．因 $2\mid 4$，故$(2)\supset(4)$，但 $2\,\overline{\in}\,(4)$，从而$(2)\not\subset(4)$．

7)　不正确．$(2,4,8,16)=(2)$(见本题 5))．

8)　不正确．例，$\mathbb{Q}[x]$是主理想环，$\mathbb{Z}[x]$是$\mathbb{Q}[x]$的子整环，但$\mathbb{Z}[x]$不是主理想环．

9)　不正确．例，整环$\mathbb{Z}[\sqrt{3}\,\mathrm{i}]$的子整环 $\mathbb{Z}$ 是主理想环，但$\mathbb{Z}[\sqrt{3}\,\mathrm{i}]$不是唯一分解环，从而$\mathbb{Z}[\sqrt{3}\,\mathrm{i}]$不是主理想环．

10)　①　正确．事实上，因 $b\mid a$，故 $\exists c\in I$，使得 $a=bc$，从而$\phi(a)=\phi(bc)=\phi(b)\phi(c)$，其中$\phi(c)\in\bar{I}$，所以$\phi(b)\mid\phi(a)$．

②　正确．事实上，因 a,b 相伴，故 $a\mid b$，$b\mid a$．由上面①，$\phi(a)\mid\phi(b)$，$\phi(b)\mid\phi(a)$，所以$\phi(a)$，$\phi(b)$相伴．

③ 不正确．例，$\phi: n \to 0$ 是整数环 $\mathbb{Z}$ 到零环$\{0\}$的一个同态满射．2 是 $\mathbb{Z}$ 的素元，但 $\phi(2)=0$ 不是零环$\{0\}$的素元．

④ 不正确．例，$\phi: a \to [a]$是 $\mathbb{Z}$ 到 $\mathbb{Z}_5$ 的同态满射．$U=\{1,-1\}$，$\overline{U}=\{[1],[2],[3],[4]\}$．$\phi: 1 \to [1], -1 \to [-1]=[4]$．[2]在$\phi$下的逆象$\notin U$．从而$\phi$不是 U 到 $\overline{U}$ 的一个同态满射．

2. 设 I 是整环．$p,a,b \in I$ 且 $p \neq 0$，$p \neq$ 单位．若 $p \mid ab$，有 $p \mid a$ 或 $p \mid b$．证明：p 是素元．

证 设 a 是 p 的任一因子，只需证明 a 是单位或 a 是 p 的相伴元．因 $a \mid p$，故 $\exists b \in I$，使得 $p=ab$．显然 $p \mid ab$．由已知，$p \mid a$ 或 $p \mid b$．若 $p \mid a$，又 $a \mid p$，从而 a 是 p 的相伴元；若 $p \mid b$，则 $\exists c \in I$，使得 $b=cp$，从而 $p=ab=acp$．因 $p \neq 0$，由消去律，$1=ac$，于是 a 是单位．因此 p 只有平凡因子．所以 p 是素元．

注 1) 本命题的逆命题不成立．即：设 I 是整环，$p,a,b \in I$ 且 p 是 I 的素元．若 $p \mid ab$，但未必有 $p \mid a$ 或 $p \mid b$．

例 $\mathbb{Z}[\sqrt{3}\,\mathrm{i}]$是整环，取 $2, 1+\sqrt{3}\,\mathrm{i}, 1-\sqrt{3}\,\mathrm{i} \in \mathbb{Z}[\sqrt{3}\,\mathrm{i}]$，2 是素元．$2 \mid 4=(1+\sqrt{3}\mathrm{i})(1-\sqrt{3}\mathrm{i})$，但 $2 \nmid 1+\sqrt{3}\,\mathrm{i}$ 且 $2 \nmid 1-\sqrt{3}\,\mathrm{i}$．这是因为，$2, 1+\sqrt{3}\,\mathrm{i}, 1-\sqrt{3}\,\mathrm{i}$ 都是素元，$2 \neq$ 单位，2 不是 $1+\sqrt{3}\,\mathrm{i}$ 与 $1-\sqrt{3}\,\mathrm{i}$ 的相伴元，所以 $2 \nmid 1+\sqrt{3}\,\mathrm{i}$ 且 $2 \nmid 1-\sqrt{3}\,\mathrm{i}$．

2) 当 I 是唯一分解环时，本命题的逆命题成立．

3. 设 I 是唯一分解环，$a \in I$，$a \neq 0$，$a \neq$ 单位，且 $a=p_1^{h_1}p_2^{h_2}\cdots p_n^{h_n}$，其中 $p_1,p_2,\cdots,p_n$ 是 n 个两两互不相伴的素元，$h_1,h_2,\cdots,h_n$ 都是正整数．又设 $b \in I$．证明：

$$b \mid a \Leftrightarrow b=\varepsilon p_1^{k_1}p_2^{k_2}\cdots p_n^{k_n},$$

其中 ε 是单位，且 $0 \leqslant k_i \leqslant h_i$，$i=1,2,\cdots,n$.

证 ($\Leftarrow$) 因

$$\begin{aligned}a &= p_1^{h_1}p_2^{h_2}\cdots p_n^{h_n} = (\varepsilon p_1^{k_1}p_2^{k_2}\cdots p_n^{k_n})(\varepsilon^{-1}p_1^{h_1-k_1}p_2^{h_2-k_2}\cdots p_n^{h_n-k_n}) \\ &= b(\varepsilon^{-1}p_1^{h_1-k_1}p_2^{h_2-k_2}\cdots p_n^{h_n-k_n}),\end{aligned}$$

其中 $\varepsilon^{-1}p_1^{h_1-k_1}p_2^{h_2-k_2}\cdots p_n^{h_n-k_n} \in I$，故 $b \mid a$.

($\Rightarrow$) 已知 $b \mid a$，因 $a \neq 0$，故 $b \neq 0$．若 b 是单位或 b 是 a 的相伴元，则命题显然成立．下面证明，$b \neq$ 单位且 $b \neq a$ 的相伴元时，命题也成立．因 $b \mid a$，故 $\exists c \in I$，使得 $a=bc$．因 $a \neq 0$，故 $c \neq 0$；因 $b \neq a$ 的相伴元，故 $c \neq$ 单位．因 I 是唯一分解环，故 b 与 c 都有唯一分解．设 b 与 c 的分解式中有 m 个两两互不相伴的素元 $q_1,q_2,\cdots,q_m$，则 $b=\varepsilon_b q_1^{s_1}q_2^{s_2}\cdots q_m^{s_m}$，$c=\varepsilon_c q_1^{t_1}q_2^{t_2}\cdots q_m^{t_m}$，其中 $\varepsilon_b,\varepsilon_c$ 是单位，s_j,t_j 都是非负整数，显然 s_j+t_j 是正整数，$j=1,2,\cdots,m$．由 $a=bc$，有

$$a=p_1^{h_1}p_2^{h_2}\cdots p_n^{h_n}=\varepsilon_b\varepsilon_c q_1^{s_1+t_1}q_2^{s_2+t_2}\cdots q_m^{s_m+t_m}.$$

因 I 是唯一分解环，故 $n=m$，且适当调换 q_i 的次序，可使 $q_i=\varepsilon_i p_i$，其中 ε_i 是单位，还有 $h_i=s_i+t_i$，$i=1,2,\cdots,n$．于是

$$b=\varepsilon_b(\varepsilon_1 p_1)^{s_1}(\varepsilon_2 p_2)^{s_2}\cdots(\varepsilon_n p_n)^{s_n}=\varepsilon_b\varepsilon_1^{s_1}\varepsilon_2^{s_2}\cdots\varepsilon_n^{s_n}p_1^{s_1}p_2^{s_2}\cdots p_n^{s_n},$$

其中 $\varepsilon_b\varepsilon_1^{s_1}\varepsilon_2^{s_2}\cdots\varepsilon_n^{s_n}=\varepsilon$ 是单位．因 $t_i \geqslant 0$，故 $0 \leqslant s_i \leqslant h_i$，$i=1,2,\cdots,n$．所以命题得证．

4. 设 I 是整环，证明：

I 是唯一分解环 $\Leftrightarrow$ 1)　$\forall a\in I, a\neq 0, a\neq$ 单位，a 有分解 $a=p_1p_2\cdots p_r$，其中 $p_1,p_2,\cdots,p_r$ 都是 I 的素元．

2)　I 中任意两个元在 I 里都有最大公因子．

证　($\Rightarrow$)　略．

($\Leftarrow$)　只需证明：$\forall a,b,p\in I$，p 是素元，若 $p\mid ab$，则 $p\mid a$ 或 $p\mid b$①．为此，先做两个准备工作．已知 I 是整环，I 中任二元在 I 里都有最大公因子．$\forall a,b,c\in I$，记 a,b 的最大公因子为 (a,b)，$\sim$ 表示相伴，则

①　$((a,b),c)\sim(a,(b,c))$．

事实上，设 $d=((a,b),c)$，则 $d\mid(a,b)$，$d\mid c$，即 $d\mid a$，$d\mid b$，$d\mid c$，从而 $d\mid a$，且 $d\mid(b,c)$，因此 $d\mid(a,(b,c))$．同理 $(a,(b,c))\mid((a,b),c)$．所以 $((a,b),c)\sim(a,(b,c))$．

②　$(ac,bc)\sim(a,b)c$．

事实上，若 a,b 不全为 0 且 $c\neq 0$．设 $d=(a,b)$，$t=(ac,bc)$，则 $d\mid a$，$d\mid b$，即 $dc\mid ac$，$dc\mid bc$，从而 $dc\mid(ac,bc)=t$，即 $\exists s\in I$，使得 $t=sdc$．下面只需证明 s 是单位．因 $t\mid ac$，$t\mid bc$，故 $\exists u,v\in I$，使得 $ac=ut$，$bc=vt$，从而 $ac=usdc$，$bc=vsdc$．因 $c\neq 0$，故由消去律，$a=usd$，$b=vsd$，于是 $sd\mid a$，$sd\mid b$，即 $sd\mid(a,b)=d$．因此 $\exists g\in I$，使得 $d=gsd$．因 a,b 不全为 0，故 $d\neq 0$，由消去律，$1=gs$，从而 s 是单位．所以 $(ac,bc)\sim dc=(a,b)c$．若 a,b 全为 0 或 $c=0$，由 $(0,0)\sim 0$ 知命题成立．

下面证明，若 p 是素元，$p\mid ab$，则 $p\mid a$ 或 $p\mid b$．因 $p\mid ab$，故 p 是 p 与 ab 的一个最大公因子．我们断言 p 与 a 不互素或 p 与 b 不互素．事实上，若 p 与 a 互素且 p 与 b 互素，则由 $p\mid pb$ 及准备工作①，②知

$$(p,ab)\sim((p,pb),ab)\sim(p,(pb,ab))\sim(p,(p,a)b)\sim(p,1\cdot b)\sim(p,b)\sim 1,$$

从而 p 与 ab 互素．因素数 p 不是单位，故此与 p 是 p 与 ab 的一个最大公因子矛盾．所以 p 与 a 不互素或 p 与 b 不互素．又因 p 是素元，故 p 是 p 与 a 的一个最大公因子或 p 是 p 与 b 的一个最大公因子，于是 $p\mid a$ 或 $p\mid b$．所以 I 是唯一分解环．

5. 设 $\mathbb{Z}[\sqrt{5}\,\mathrm{i}]=\{a+b\sqrt{5}\,\mathrm{i}\mid a,b\in\mathbb{Z}\}$ 是整环．证明：

1)　ε 是 $\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$ 的单位 $\Leftrightarrow|\varepsilon|^2=1\Leftrightarrow\varepsilon=\pm 1$．

2)　若 $\alpha\in\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$，$|\alpha|^2=9$，则 α 是素元．

3)　9 在 $\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$ 里有不同的分解．

4)　$\alpha=3(2+\sqrt{5}\,\mathrm{i})$，$\beta=(2+\sqrt{5}\,\mathrm{i})(2-\sqrt{5}\,\mathrm{i})$ 在 $\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$ 里没有最大公因子．

5)　若 p 是素元，$p\mid ab$，但未必有 $p\mid a$ 或 $p\mid b$．

证　1)　ε 是单位 $\Rightarrow|\varepsilon|^2=1$．

事实上，设 $\varepsilon=a+b\sqrt{5}\,\mathrm{i}$ 是单位，则 $\exists\varepsilon^{-1}=c+d\sqrt{5}\,\mathrm{i}\in\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$，使得 $1=\varepsilon\varepsilon^{-1}$，即 $1=|\varepsilon\varepsilon^{-1}|^2=|\varepsilon|^2|\varepsilon^{-1}|^2$，从而 $1=(a^2+5b^2)(c^2+5d^2)$．因 a^2+5b^2，c^2+5d^2 都是正整数，故

① 张禾瑞．近世代数基础．北京：高等教育出版社，1978．131．定理 2．

$a^2+5b^2=1$，即$|\varepsilon|^2=1$.

$$|\varepsilon|^2=1\Rightarrow\varepsilon=\pm 1.$$

事实上，设$\varepsilon=a+b\sqrt{5}\,\mathrm{i}$，$|\varepsilon|^2=a^2+5b^2=1$，$a,b\in\mathbb{Z}$．若$b\neq 0$，则因$a^2$是非负整数，$5b^2$是大于或等于5的整数，故$a^2+5b^2\neq 1$，发生矛盾．所以$b=0$．于是$a^2=1$，即$a=\pm 1$，从而$\varepsilon=a+b\sqrt{5}\,\mathrm{i}=\pm 1$.

$$\varepsilon=\pm 1\Rightarrow\varepsilon\text{是单位}.$$

事实上，$\varepsilon=\pm 1$有逆元$\pm 1\in\mathbb{Z}[\sqrt{5}\mathrm{i}]$，所以$\varepsilon$是单位．

2) 因$|\alpha|^2=9$，故$\alpha\neq 0$，$\alpha\neq$单位．设$\beta=u+v\sqrt{5}\,\mathrm{i}\in\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$，$\beta$是$\alpha$的任一因子，则$\exists\gamma\in\mathbb{Z}[\sqrt{5}\mathrm{i}]$，使得$\alpha=\beta\gamma$．从而$|\alpha|^2=|\beta|^2|\gamma|^2$，即$9=(u^2+5v^2)|\gamma|^2$．因$u^2+5v^2\neq 3$，故$|\beta|^2=1$或9．当$|\beta|^2=1$时，$\beta$是单位；当$|\beta|^2=9$时，$|\gamma|^2=1$，即$\gamma$是单位．因此$\beta=\alpha\gamma^{-1}$，其中$\gamma^{-1}$是单位，从而$\beta$是$\alpha$的相伴元．于是$\alpha$只有平凡因子．所以$\alpha$是素元．

3) $9=3\cdot 3=(2+\sqrt{5}\,\mathrm{i})(2-\sqrt{5}\,\mathrm{i})$．其中$|3|^2=|2\pm\sqrt{5}\,\mathrm{i}|^2=9$．由2)知，$3$，$2\pm\sqrt{5}\,\mathrm{i}$都是素元．又$2\pm\sqrt{5}\,\mathrm{i}\neq(\pm 1)3$，即$2\pm\sqrt{5}\,\mathrm{i}$都不是3的相伴元．所以9在$\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$里有不同的分解.

4) 因$\alpha=3(2+\sqrt{5}\,\mathrm{i})$，$\beta=(2+\sqrt{5}\,\mathrm{i})(2-\sqrt{5}\,\mathrm{i})=3\cdot 3$，故$\alpha,\beta$的所有的公因子是$\pm 1$，$\pm 3$，$\pm(2+\sqrt{5}\,\mathrm{i})$．因$\pm 3$，$\pm(2+\sqrt{5}\,\mathrm{i})$都是素元，且$\pm 3$与$\pm(2+\sqrt{5}\,\mathrm{i})$不相伴，故$2+\sqrt{5}\,\mathrm{i}\nmid\pm 3$，$3\nmid\pm(2+\sqrt{5}\,\mathrm{i})$，从而$\pm 3$与$\pm(2+\sqrt{5}\,\mathrm{i})$都不是$\alpha,\beta$的最大公因子．又因$\pm 1$是单位，3不等于单位，故$3\nmid\pm 1$，从而$\pm 1$也不是$\alpha,\beta$的最大公因子．所以$\alpha,\beta$无最大公因子．

5) 例，3是$\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$的素元，且$3\,|\,9=(2+\sqrt{5}\,\mathrm{i})(2-\sqrt{5}\,\mathrm{i})$．但$3\nmid 2+\sqrt{5}\,\mathrm{i}$且$3\nmid 2-\sqrt{5}\mathrm{i}$.

注 1) 类似于本命题中2)的证法，可证：

① 若$\alpha\in\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$，$|\alpha|^2=49$，则$\alpha$是素元．

② 若$\alpha\in\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$，$|\alpha|^2=21$，则$\alpha$是素元．

③ 若$\alpha\in\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$，$|\alpha|^2=4$，则$\alpha$是素元．

④ 若$\alpha\in\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$，$|\alpha|^2=6$，则$\alpha$是素元．

2) 21在$\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$中分解不唯一，因

$$21=3\cdot 7=(1+2\sqrt{5}\,\mathrm{i})(1-2\sqrt{5}\,\mathrm{i})=(4+\sqrt{5}\,\mathrm{i})(4-\sqrt{5}\,\mathrm{i}),$$

其中$3,7,1\pm 2\sqrt{5}\,\mathrm{i},4\pm\sqrt{5}\,\mathrm{i}$都是$\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$的素元（由注1)知）且它们互不相伴．

6在$\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$中分解也不唯一．因

$$6=2\cdot 3=(1+\sqrt{5}\,\mathrm{i})(1-\sqrt{5}\,\mathrm{i})$$

由注1)知，$2,3,1\pm\sqrt{5}\,\mathrm{i}$都是$\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$的素元且它们互不相伴．

3) 类似于本命题中4)的证法，可证：$\alpha=6=2\cdot 3=(1+\sqrt{5}\,\mathrm{i})(1-\sqrt{5}\,\mathrm{i})$，$\beta=3+3\sqrt{5}\,\mathrm{i}=3(1+\sqrt{5}\,\mathrm{i})$在$\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$里无最大公因子（参看第十四章，一，8）.

4) 2是$\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$的素元，且$2\,|\,6=(1+\sqrt{5}\,\mathrm{i})(1-\sqrt{5}\,\mathrm{i})$．但$2\nmid 1+\sqrt{5}\,\mathrm{i}$，$2\nmid 1-\sqrt{5}\,\mathrm{i}$.

四、思考问题

1. 设 I 是整环，a 是 I 的幂零元（第九章，四，12），$\varepsilon\in I$. 证明：

$$\varepsilon+a \text{ 是 } I \text{ 的单位} \Leftrightarrow \varepsilon \text{ 是 } I \text{ 的单位}.$$

2. 证明：相伴是整环 I 的元间的一个等价关系．写出 I 的等价类．

3. 举例说明，在整环 I 中，非零非单位的元未必有分解．

4. 1)　在整环 $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$ 中，证明：

①　设 $\varepsilon=a+b\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$，则

$$\varepsilon \text{ 是 } \mathbb{Z}[\sqrt{2}] \text{ 的单位} \Leftrightarrow \varepsilon\bar{\varepsilon}=a^2-2b^2=\pm 1.$$

②　设 $\alpha=a+b\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$，则

$$\alpha\bar{\alpha}=a^2-2b^2 \text{ 是 } \mathbb{Z} \text{ 的素数} \Rightarrow \alpha \text{ 是 } \mathbb{Z}[\sqrt{2}] \text{ 的素元}.$$

③　7 不是 $\mathbb{Z}[\sqrt{2}]$ 的素元．

④　在 $\mathbb{Z}[\sqrt{2}]$ 中有无限多个不同的单位．

2)　在整环 $\mathbb{Z}[\sqrt{10}]=\{a+b\sqrt{10}\mid a,b\in\mathbb{Z}\}$ 中，证明：

①　设 $\varepsilon=a+b\sqrt{10}\in\mathbb{Z}[\sqrt{10}]$，则

$$\varepsilon \text{ 是 } \mathbb{Z}[\sqrt{10}] \text{ 的单位} \Leftrightarrow \varepsilon\bar{\varepsilon}=a^2-10b^2=\pm 1.$$

②　$2,3,4+\sqrt{10},4-\sqrt{10}$ 是 $\mathbb{Z}[\sqrt{10}]$ 中互不相伴的素元．

③　$6(\in\mathbb{Z}[\sqrt{10}])$ 的分解不唯一．

5. 设 $S_p=\left\{\frac{a}{b}\in\mathbb{Q}\;\middle|\;a,b\in\mathbb{Z},p\nmid b\right\}$，$p$ 是素数．证明：S_p 是主理想环．

6. 设 I 是主理想环，$a,b,c\in I$，证明：

1)　若 a,b 互素且 $a\mid bc$，则 $a\mid c$.

2)　若 a,b 互素且 $a\mid c,b\mid c$，则 $ab\mid c$.

3)　若 p 是 I 的素元，则 $p\mid a$ 或 p,a 互素．

4)　若 p_1,p_2 是 I 的素元且 p_1,p_2 不相伴，$p_1\mid a,p_2\mid a$，则 $p_1p_2\mid a$.

7. 设 I 是主理想环．取定 $a\in I$. 证明：

1)　设 I 的模理想 (a) 的剩余类 $[b]=b+(a)$ 中的 b 与 a 互素，则 $[b]$ 中的任一元都与 a 互素．

2)　$G=\{[b]\in I/(a)\mid b\in I,b,a \text{ 互素}\}$ 对于 I 的模理想 (a) 的剩余类环 $I/(a)$ 的乘法来说作成一个群．

8. 设 I 是主理想环，$0\neq a\in I$. 证明：只有有限个理想包含 a.

第十五章　欧氏环、多项式环的因子分解

一、基本问题问答

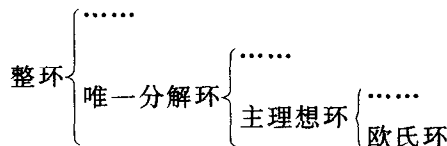
1. 回答下列各问题．

1）　欧氏环必存在吗？

2）　欧氏环、主理想环与唯一分解环三者的关系是什么？

答　1）　欧氏环必存在．如整数环 $\mathbb{Z}$ 和域 F 上一元多项式环 $F[x]$ 都是欧氏环．而欧氏环的概念正是从 $\mathbb{Z}$ 和 $F[x]$ 中都能做带余除法这种共性抽象出来的．

2）　欧氏环必为主理想环，主理想环必为唯一分解环．反之不对．唯一分解环未必是主理想环，例，$\mathbb{Z}[x]$ 是唯一分解环，但 $\mathbb{Z}[x]$ 不是主理想环．主理想环未必是欧氏环，例，设 $\alpha=\dfrac{1+\sqrt{-19}}{2}$，则 $\mathbb{Z}[\alpha]$ 是主理想环，但 $\mathbb{Z}[\alpha]$ 不是欧氏环（证明略）．唯一分解环的范围比主理想环的范围大，主理想环的范围比欧氏环的范围大．如图示：



2. 关于命题：设 $I[x]$ 是整环 I 上的一元多项式环，$g(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0\in I[x]$，且 a_n 是单位，则 $\forall f(x)\in I[x]$，$\exists q(x),r(x)\in I[x]$，使得

$$f(x)=q(x)g(x)+r(x)$$

且 $r(x)=0$ 或 $\deg r(x)<\deg g(x)$①.

1）　$I=\{0\}$ 时，命题还成立吗？

2）　将 a_n 是单位改为 $a_n\neq 0$，行不行？

3）　$q(x),r(x)$ 是否分别唯一？

4）　命题的作用是什么？

答　1）　显然成立．因此，只需证明 $I\neq\{0\}$ 时，命题成立．

2）　不行．因为，$a_n(\neq 0)\in$ 整环 I，未必 $\exists a_n^{-1}\in I$，就不能把 $f(x)$ 的次数降下来．当 I 是域时，只要 $a_n(\neq 0)\in I$，a_n 就是单位，因此命题成立．

3）　$q(x),r(x)$ 都唯一．事实上，设

$$f(x)=q(x)g(x)+r(x),\quad r(x)=0\text{ 或 }\deg r(x)<\deg g(x),$$

$$f(x)=q_1(x)g(x)+r_1(x),\quad r_1(x)=0\text{ 或 }\deg r_1(x)<\deg g(x).$$

① 张禾瑞．近世代数基础．北京：高等教育出版社，1978. 140. 引理．

则$[q(x)-q_1(x)]g(x)=r_1(x)-r(x)$. 若 $r_1(x)-r(x)\neq 0$,则 $q(x)-q_1(x)\neq 0$,由第十一章,四,1,10)及 $\deg(q(x)-q_1(x))\geqslant 0$,得

$$\deg(r_1(x)-r(x)) = \deg\left[(q(x)-q_1(x))g(x)\right]$$
$$= \deg(q(x)-q_1(x)) + \deg g(x) \geqslant \deg g(x) >$$
$$\max(\deg r_1(x), \deg r(x)) \geqslant \deg(r_1(x)-r(x)).$$

即 $\deg(r_1(x)-r(x))>\deg(r_1(x)-r(x))$,此为矛盾. 从而 $r_1(x)-r(x)=0$,即 $r_1(x)=r(x)$. 因 I 无零因子,故由$[q(x)-q_1(x)]g(x)=r_1(x)-r(x)=0$,$g(x)\neq 0$,有 $q(x)-q_1(x)=0$,即 $q_1(x)=q(x)$.

4) 证明一般域 F 上的一元多项式环 $F[x]$是一个欧氏环要用该命题. 该命题实际上是数域 F 上的一元多项式环 $F[x]$中带余除法定理的推广. 因此十分重要. 后面还要用到. 将多项式 $q(x)$,$r(x)$分别称为 $f(x)$除以 $g(x)$所得的商式和余式,$f(x)$称为被除式,$g(x)$称为除式.

注　该命题可对 $f(x)$的次数用数学归纳法证明.

3. 不可约多项式与可约多项式的定义是什么?

答　设 I 是整环,定义:

$p(x)$是 $I[x]$的不可约多项式 $\Leftrightarrow$ $p(x)$是 $I[x]$的素元

$\Leftrightarrow$ $p(x)\in I[x]$,$p(x)\neq 0$,$p(x)\neq I[x]$的单位,$p(x)$在 $I[x]$中只有平凡因子.

$f(x)$是 $I[x]$的可约多项式

$\Leftrightarrow$ $f(x)$不是 $I[x]$的不可约多项式,$f(x)\neq 0$,$f(x)\neq I[x]$的单位

$\Leftrightarrow$ $f(x)\in I[x]$,$f(x)\neq 0$,$f(x)\neq I[x]$的单位,$f(x)$在 $I[x]$中有真因子.

注　1)　若 $f(x)$不是 $I[x]$的不可约多项式,则 $f(x)$未必是 $I[x]$的可约多项式,因为 $f(x)$还可能$=0$,或是 $I[x]$的单位.

2)　设 $f(x)$,$g(x)$,$h(x)\in I[x]$,若 $f(x)=g(x)h(x)$,未必 $f(x)$在 I 上可约. 例,虽 $x-1=(-1)(-x+1)$,但 $x-1$ 在 $\mathbb{Z}$ 上不可约. 见第十四章,一,6.

4. 证明:设 I 是唯一分解环,$f(x)\in I[x]$,若 $f(x)$可约且本原,则 $f(x)=g(x)h(x)$,其中 $g(x)$,$h(x)\in I[x]$,$0<\deg g(x)<\deg f(x)$,$0<\deg h(x)<\deg f(x)$①.

证　因 $f(x)$可约,故 $f(x)$有真因子 $g(x)\in I[x]$,使得 $f(x)=g(x)h(x)$. 且 $h(x)(\in I[x])$也是 $f(x)$的真因子②. 因 $f(x)\neq 0$,故 $g(x)\neq 0$,$h(x)\neq 0$. 断言 $\deg g(x)>0$. 不然,若 $\deg g(x)=0$,则 $g(x)=c\in I$,从而 $f(x)=\text{ch}(x)$,即 c 是 $f(x)$的系数的公因子. 因 $f(x)$本原,故 $g(x)=c$ 是单位,此与 $g(x)$是 $f(x)$的真因子矛盾. 所以,$\deg g(x)>0$. 同理,$\deg h(x)>0$. 由第十一章,四,1,10),$\deg f(x)=\deg g(x)+\deg h(x)$. 于是 $\deg g(x)<\deg f(x)$,$\deg h(x)<\deg f(x)$.

注　1)　该命题的逆命题不正确. 即,设 I 是唯一分解环,$f(x)\in I[x]$,若 $f(x)=g(x)h(x)$,其中 $g(x)$,$h(x)\in I[x]$,$0<\deg g(x)<\deg f(x)$,$0<\deg h(x)<\deg f(x)$,则 $f(x)$可约但未必本原. 例,$\mathbb{Z}$ 是唯一分解环,$4x^2-4\in\mathbb{Z}[x]$,$4x^2-4=(2x+2)(2x-2)$,其中 $2x+2$,$2x-2\in\mathbb{Z}[x]$,$0<\deg(2x+2)=1<\deg(4x^2-4)$,$0<\deg(2x-2)=1<\deg(4x^2-4)$,虽

---

① 张禾瑞. 近世代数基础. 北京:高等教育出版社,1978. 142. (C).

② 同上. 127. 推论.

$4x^2-4$ 可约，但$4x^2-4$非本原．

2） 该命题中，条件 $f(x)$本原不可去掉．例，$\mathbb{Z}$是唯一分解环，$2x+2\in\mathbb{Z}[x]$，因 $x+1$ 是 $2x+2$ 的真因子，故 $2x+2$ 可约，但非本原．虽有 $2x+2=2(x+1)$，其中 $2,x+1\in\mathbb{Z}[x]$，但 $\deg 2=0,\deg(x+1)=1=\deg(2x+2)$.

3） 设 F 是域，$f(x)\in F[x]$，则

$f(x)$可约 $\Leftrightarrow f(x)=g(x)h(x)$，其中 $g(x),h(x)\in F[x]$，

$$0<\deg g(x)<\deg f(x),\ 0<\deg h(x)<\deg f(x).$$

事实上，($\Rightarrow$) 因 $f(x)$可约，故 $f(x)\neq 0$. 而域 F 上非零多项式都本原，从而由该命题知结论成立．($\Leftarrow$) 因 $f(x)=g(x)h(x)$，$g(x),h(x)$都不是单位，且 $f(x)\neq 0$，故 $f(x)$有真因子，$f(x)$显然不是单位，所以 $f(x)$可约．

4） 由该命题直接可知：设 I 是唯一分解环，$f(x)\in I[x]$，若 $f(x)$可约且本原，则 $\deg f(x)>0$.

5. 证明命题：设 I 是唯一分解环，$f(x),g(x),h(x)\in I[x]$且 $f(x)=g(x)h(x)$，则

$$f(x)\text{ 本原}\Leftrightarrow g(x),\ h(x)\text{ 都本原}$$[1]．

证 ($\Rightarrow$) (反证法)假定 $g(x)$非本原，则 $g(x)$的系数的最大公因子 $c\neq$单位．由$f(x)=g(x)h(x)$和 c 是 $f(x)$的系数的公因子，从而 $f(x)$非本原，与已知矛盾．若 $h(x)$非本原，同样得矛盾．所以 $g(x),h(x)$都本原．

($\Leftarrow$) (反证法)若 $f(x)$非本原，则 $f(x)$的系数的一个最大公因子 $d\neq$单位，且 $f(x)=df_0(x)$，从而 $df_0(x)=g(x)h(x)$. 因 $g(x),h(x)$都本原，故 $g(x)\neq 0,h(x)\neq 0$. 因 $I[x]$无零因子，故 $f(x)=g(x)h(x)\neq 0$，于是 $d\neq 0$. 因 I 是唯一分解环，故 $\exists I$ 的素元 p，使得 $p\mid d$，即 $\exists q\in I$，使得 $d=pq$. 从而 $pqf_0(x)=g(x)h(x)$，即 $p\mid q(x)h(x)$. 因 p 是 I 的素元，故 p 必为 $I[x]$的素元(见后第十五章，一，9，2))．所以 $p\mid g(x)$或 $p\mid h(x)$. 若 $p\mid g(x)$，则 p 是 $g(x)$的系数的公因子，此与 $g(x)$本原矛盾；若 $p\mid h(x)$，则 p 是 $h(x)$的系数的公因子，此与 $h(x)$本原矛盾．因此 $f(x)$本原．

注 1） 该命题可推广成：设 I 是唯一分解环，$f(x),q_1(x),q_2(x),\cdots,q_r(x)\in I[x]$且 $f(x)=q_1(x)q_2(x)\cdots q_r(x)$，则

$$f(x)\text{ 本原}\Leftrightarrow\text{每 }q_i(x)\text{ 本原},\ i=1,2,\cdots,r.$$

2） 该命题称为高斯(Gauss)引理．

6. 给出下面命题：设 Q 是唯一分解环 I 的商域，$f(x)\in Q[x]$，$f(x)\neq 0$，则

(i) $f(x)=\dfrac{b}{a}f_0(x)$，其中 $a(\neq 0),b\in I$，$f_0(x)$在 $I[x]$中本原．

(ii) 若 $f(x)=\dfrac{d}{c}g_0(x)$，其中 $c(\neq 0),d\in I$，$g_0(x)$在 $I[x]$中本原，有 $g_0(x)=\varepsilon f_0(x)$，其中 ε 是 I 的单位[2].

1） 该命题的作用为何？

2） 该命题本身说明什么？

---

① 张禾瑞．近世代数基础．北京：高等教育出版社，1978．142．引理 1.

② 同上．143．引理 2.

3）　与该命题类似地证明：设 I 是唯一分解环，$f(x)(\neq 0)\in I[x]$，则

①　$f(x)=df_0(x)$，其中 $d\in I$，$f_0(x)$ 在 $I[x]$ 中本原．

②　若 $f(x)=bg_0(x)$，其中 $b\in I$，$g_0(x)$ 在 $I[x]$ 中本原，有 $g_0(x)=\varepsilon f_0(x)$，其中 ε 是 I 的单位．

答　1）　设 I 是唯一分解环，则 I 有商域 Q，想利用 $Q[x]$ 是唯一分解环且 $Q[x]\supset I[x]$，来解决 $I[x]$ 也是唯一分解环，因此首先给出该命题．

2）　①　说明商域 Q 上的多项式总可以用唯一分解环 I 上的本原多项式来表示．一般多项式总可以转化为本原多项式．

②　设 Q 是唯一分解环 I 的商域，$f_0(x)$，$g_0(x)$ 是 $I[x]$ 中的本原多项式，则

$f_0(x)$，$g_0(x)$ 在 $Q[x]$ 中相伴 $\Leftrightarrow$ $f_0(x)$，$g_0(x)$ 在 $I[x]$ 中相伴．

3）　**证**　①　设 $f(x)=a_0+a_1x+\cdots+a_nx^n\neq 0$. 因 I 是唯一分解环，故 $a_0,a_1,\cdots,a_n$ 有最大公因子，设其中一个是 d，显然 $d\neq 0$. 于是 $\exists b_i\in I$，使得 $a_i=db_i$，$i=0,1,2,\cdots,n$. 由第十四章，二，5，$b_0,b_1,\cdots,b_n$ 互素，从而

$$f(x)=d(b_0+b_1x+\cdots+b_nx^n)=df_0(x),$$

其中 $f_0(x)=b_0+b_1x+\cdots+b_nx^n$ 在 $I[x]$ 中本原．

②　由已知，$f(x)=df_0(x)=bg_0(x)$，其中 $d,b\in I$，$f_0(x)$，$g_0(x)$ 在 $I[x]$ 中本原．设

$$f(x)=a_0+a_1x+\cdots+a_nx^n,$$
$$f_0(x)=s_0+s_1x+\cdots+s_nx^n,$$
$$g_0(x)=t_0+t_1x+\cdots+t_nx^n.$$

则 $a_i=ds_i=bt_i$，$i=0,1,2,\cdots,n$. 因 $s_0,s_1,\cdots,s_n$ 互素，$t_0,t_1,\cdots,t_n$ 互素，又 $d\neq 0$，$b\neq 0$，故由第十四章，二，5，d 与 b 都是 $a_0,a_1,\cdots,a_n$ 的最大公因子．从而 $\exists I$ 的单位 ε，使得 $d=b\varepsilon$，于是 $bg_0(x)=b\varepsilon f_0(x)$. 因 $b\neq 0$，故由消去律，$g_0(x)=\varepsilon f_0(x)$，其中 ε 是单位．即除差单位因子外，$f(x)$ 的表法：$f(x)=df_0(x)$ 唯一．

7. 关于命题：设 Q 是唯一分解环 I 的商域，$f_0(x)$ 在 $I[x]$ 中本原，则

$f_0(x)$ 在 $I[x]$ 中可约 $\Leftrightarrow$ $f_0(x)$ 在 $Q[x]$ 中可约①．

1）　若去掉条件"$f_0(x)$本原"，命题是否仍成立？

2）　若将商域 Q 改为包含唯一分解环 I 的域，命题是否仍成立？

3）　设 Q 是唯一分解环 I 的商域，$f_0(x)\in I[x]$. 若 $f_0(x)$ 在 $I[x]$ 中本原，则 $f_0(x)$ 在 $Q[x]$ 中也本原吗？反之，对吗？

答　1）　不成立．例，有理数域 $\mathbb{Q}$ 是唯一分解环 $\mathbb{Z}$ 的商域，6 在 $\mathbb{Z}[x]$ 中非本原．因 $6\neq 0$，$6\neq\mathbb{Z}[x]$ 的单位，6 在 $\mathbb{Z}[x]$ 中有真因子 2，故 6 在 $\mathbb{Z}[x]$ 中可约，但 6 在 $\mathbb{Q}[x]$ 中不可约，这是因为 6 是 $\mathbb{Q}[x]$ 的单位．由第十五章，二，4，命题的充分性成立．

2）　不成立．例，实数域 $\mathbf{R}$ 是包含唯一分解环 $\mathbb{Z}$ 的域，但 $\mathbf{R}$ 不是 $\mathbb{Z}$ 的商域．x^2-2 在 $\mathbb{Z}[x]$ 中本原．x^2-2 在 $\mathbf{R}[x]$ 中可约，而 x^2-2 在 $\mathbb{Z}[x]$ 中不可约．

3）　若 $f_0(x)$ 在 $I[x]$ 中本原，则 $f_0(x)$ 在 $Q[x]$ 中也本原，这是因为 $f_0(x)$ 在 $I[x]$ 中本原，从而 $f_0[x]\neq 0$，于是 $f_0(x)$ 的系数在域 Q 中的最大公因子是 Q 的非零元，即 Q 的单位．所以 $f_0(x)$ 在 $Q[x]$ 中本原．

---

①　张禾瑞．近世代数基础．北京：高等教育出版社，1978．144．引理 3．

反之,不对,例,$\mathbf{Q}$是$\mathbf{Z}$的商域,$2x+4\in\mathbf{Z}[x]$,$2x+4$在$\mathbf{Q}[x]$中本原,但$2x+4$在$\mathbf{Z}[x]$中非本原.

8. 关于命题:设I是唯一分解环,$f_0(x)$在$I[x]$中本原,$\deg f_0(x)>0$,则$f_0(x)$在$I[x]$中有唯一分解①.在证明中,

1) 若$f_0(x)$不是不可约的,那么$f_0(x)$一定是可约的吗?

2) 为何"由(A),我们可以假定$q_0^{(i)}(x)=\dfrac{b_i}{a_i}p_0^{(i)}(x)$"②?

3) 证明$f_0(x)$在$I[x]$里的分解唯一的主要思路是什么?

答 1) 未必,见第十五章,一,3,注1).但在该命题中,$f_0(x)\neq 0$,又因$\deg f_0(x)>0$,故$f_0(x)\neq I[x]$的单位,从而$f_0(x)$可约.

2) 因$Q[x]$是唯一分解环,故$f_0(x)$在$Q[x]$里有唯一分解,所以我们有$r=t$,且适当调换$q_0^{(i)}(x)$的次序可使$q_0^{(i)}(x)=\alpha_i p_0^{(i)}(x)$,其中$\alpha_i$是$Q[x]$的单位.由(A),$\alpha_i$是$Q$的单位,从而可令$\alpha_i=\dfrac{b_i}{a_i}\in Q$,其中$a_i,b_i\in I$,于是$q_0^{(i)}(x)=\dfrac{b_i}{a_i}p_0^{(i)}(x)$.

3) 主要依据上面7中命题,可将$f_0(x)$在$I[x]$里的分解看成在$Q[x]$里的分解,这里Q是I的商域.而$Q[x]$是唯一分解环,$f_0(x)$在$Q[x]$里的分解唯一,由此导出$f_0(x)$在$I[x]$里的分解唯一.

9. 关于命题:若I是唯一分解环,则$I[x]$也是.③

1) 为何"这样,我们只需看$f(x)=df_0(x)$,d不是I的单位,$f_0(x)$是次数大于零的本原多项式时的情形"④?

2) 已知p_i是I的素元,p_i为何也是$I[x]$的不可约多项式⑤?

3) 已知$q_i(\in I)$是$I[x]$的不可约多项式,q_i为何也是I的素元⑥?

4) 为何$I[x]$的不可约多项式$q_0^{(i)}(x)(\overline{\in} I)$是$I[x]$中的本原多项式⑦?

5) 换个方法来证明该命题.

答 1) 因为,我们假设$f(x)\overline{\in} I$,$f(x)$非本原,又d是$f(x)$的系数的一个最大公因子,从而d不是I的单位.因$f(x)=df_0(x)$,故$\deg f_0(x)=\deg f(x)>0$且$f_0(x)$在$I[x]$中本原(第十五章,一,6,3)).

2) 事实上,假定p_i不是$I[x]$的不可约多项式,又$p_i\neq 0$,$p_i\neq I$的单位$=I[x]$的单位,从而p_i是$I[x]$的可约多项式.于是p_i有真因子$h(x)\in I[x]$,使得$p_i=h(x)k(x)$,其中$k(x)\in I[x]$.因$p_i\neq 0$,故$h(x)\neq 0$,$k(x)\neq 0$.因此$0=\deg p_i=\deg h(x)+\deg k(x)$.而$\deg h(x)$,$\deg k(x)$是非负整数,从而$\deg h(x)=0$,即$h(x)\in I$,所以$p_i$在$I$中有真因子$h(x)$,此与$p_i$是$I$的素元矛盾.于是$p_i$在$I[x]$中不可约.

3) 事实上,假定q_i不是I的素元,又$q_i\neq 0$,$q_i\neq I[x]$的单位$=I$的单位,从而q_i在I

① 张禾瑞.近世代数基础.北京:高等教育出版社,1978.145.引理4.

② 同上.146.4行.

③ 同上.146.定理1.

④ 同上.146.13行.

⑤ 同上.146.22行.

⑥ 同上.146.25行.

⑦ 同上.146.26行.

中有真因子 b_i，$b_i \neq I$ 的单位 $= I[x]$ 的单位，$b_i \neq q_i$ 在 I 中的相伴元，因此 $b_i \neq q_i$ 在 $I[x]$ 中的相伴元．于是 $b_i(\in I[x])$ 也是 q_i 在 $I[x]$ 中的真因子，此与 q_i 在 $I[x]$ 中不可约矛盾．所以 q_i 是 I 的素元．

4) 事实上，假定 $q_0^{(i)}(x)$ 在 $I[x]$ 中非本原，则 $q_0^{(i)}(x)$ 的系数的最大公因子 $d_i \neq I$ 的单位 $= I[x]$ 的单位．因 $q_0^{(i)}(x) \overline{\in} I$，即 $\deg q_0^{(i)}(x) > 0$，故 d_i 不是 $q_0^{(i)}(x)$ 在 $I[x]$ 中的相伴元，于是 d_i 是 $q_0^{(i)}(x)$ 在 $I[x]$ 中的真因子，此与 $q_0^{(i)}(x)$ 在 $I[x]$ 中不可约矛盾．所以 $q_0^{(i)}(x)$ 在 $I[x]$ 中本原．

5) 事实上，① 显然 $I[x]$ 的每一个既不是零也不是单位的元 $f(x)$ 都在 $I[x]$ 里有分解.

② 设 $p(x)$ 是 $I[x]$ 的一个不可约多项式，若 $p(x) \mid f(x)g(x)$，下面证明 $p(x) \mid f(x)$ 或 $p(x) \mid g(x)$.

如果 $f(x)$，$g(x)$ 中有一个是零多项式，结论显然成立，从而可设 $f(x) \neq 0$，$g(x) \neq 0$.

假设 $\deg p(x) > 0$，即 $p(x) \overline{\in} I$. 因 $p(x)$ 在 $I[x]$ 中不可约，故 $p(x)$ 在 $I[x]$ 里本原（见本题 4)）. 由第十五章，一，7，$p(x)$ 在 $Q[x]$ 里不可约，其中 Q 是 I 的商域．因在 $Q[x]$ 中也有 $p(x) \mid f(x)g(x)$，$Q[x]$ 是唯一分解环，故在 $Q[x]$ 中有 $p(x) \mid f(x)$ 或 $p(x) \mid g(x)$. 不妨设在 $Q[x]$ 中 $p(x) \mid f(x)$，则 $\exists f_1(x)(\neq 0) \in Q[x]$，使得 $f(x) = p(x)f_1(x)$. 由上面 6 中命题，$f_1(x) = \dfrac{b}{a} f_0(x)$，其中 $a(\neq 0)$，$b \in I$，$f_0(x)$ 是 $I[x]$ 的本原多项式．因此 $f(x) = \dfrac{b}{a} p(x) f_0(x)$，即 $af(x) = bp(x)f_0(x)$. 因 $p(x)$，$f_0(x)$ 都在 $I[x]$ 里本原，故由上面 5 中命题，$p(x)f_0(x)$ 在 $I[x]$ 里也本原．于是 b 是 $af(x)$ 的系数的最大公因子，而 a 是 $af(x)$ 的系数的公因子，从而 $a \mid b$，即 $\exists c \in I$，使得 $b = ca$，$c = \dfrac{b}{a}$，得 $f(x) = cp(x)f_0(x)$，其中 $cf_0(x) \in I[x]$. 所以，在 $I[x]$ 中有 $p(x) \mid f(x)$.

假设 $\deg p(x) = 0$，即 $p(x) = p \in I$. 因 p 在 $I[x]$ 中不可约，故 p 是 I 的素元（见本题 3)）. 由第十五章，一，6，3)，$f(x) = af_0(x)$，$g(x) = bg_0(x)$，其中 $f_0(x)$，$g_0(x)$ 都在 $I[x]$ 中本原，$a, b \in I$. 由上面 5 中命题，$f_0(x)g_0(x)$ 也在 $I[x]$ 中本原．由 $p \mid f(x)g(x)$，有 $p \mid abf_0(x)g_0(x)$，即 $\exists h(x) \in I[x]$，使得 $ph(x) = abf_0(x)g_0(x)$. 因 ab 是 $ph(x)$ 的系数的最大公因子，而 p 是 $ph(x)$ 的系数的公因子，故 $p \mid ab$. 因 p 是唯一分解环 I 的素元，故 $p \mid a$ 或 $p \mid b$，即 $p \mid af_0(x) = f(x)$ 或 $p \mid bg_0(x) = g(x)$.

综上，知 $I[x]$ 是唯一分解环[①].

注 1) 由本题 2)，3) 知：设 I 是唯一分解环，$p \in I$，则

$$p \text{ 是 } I \text{ 的素元} \Leftrightarrow p \text{ 是 } I[x] \text{ 的不可约多项式}.$$

例

5 是 $\mathbf{Z}$ 的素元 $\Leftrightarrow$ 5 是 $\mathbf{Z}[x]$ 的不可约多项式.

6 不是 $\mathbf{Z}$ 的素元 $\Leftrightarrow$ 6 不是 $\mathbf{Z}[x]$ 的不可约多项式.

5，6 都不是 $\mathbf{Q}$ 的素元 $\Leftrightarrow$ 5，6 都不是 $\mathbf{Q}[x]$ 的不可约多项式.

---

① 张禾瑞．近世代数基础．北京：高等教育出版社，1978. 131. 定理 2.

2) 由本题4)知:设 I 是唯一分解环.若 $p(x)(\overline{\in} I)$ 在 $I[x]$ 中不可约,则 $p(x)$ 在 $I[x]$ 中本原.但该命题的逆命题不成立.

例 x^2-1 在 $\mathbb{Z}[x]$ 中本原,而在 $\mathbb{Z}[x]$ 中可约.

3) 设 I 是唯一分解环.若 $p(x)$ 在 $I[x]$ 中不可约,且 $p(x)\in I$,则 $p(x)$ 未必在 $I[x]$ 中本原.

例 2 在 $\mathbb{Z}[x]$ 中不可约,但在 $\mathbb{Z}[x]$ 中非本原.

10. 证明:设 I 是唯一分解环,则 $I[x_1,x_2,\cdots,x_n]$ 也是,这里 $x_1,x_2,\cdots,x_n$ 是 I 上的无关未定元①.

证 对 n 作数学归纳法.

1) $n=1$ 时,即第十五章,一,9.

2) 假定 $n-1$ 时,命题成立,今看 n 时.因 $I[x_1,x_2,\cdots,x_n]=I[x_1,x_2,\cdots,x_{n-1}][x_n]$,由归纳假定,$I[x_1,x_2,\cdots,x_{n-1}]$ 是唯一分解环,故 $I[x_1,x_2,\cdots,x_n]$ 也是.

依归纳原理,命题得证.

二、典型问题分析

1. 证明:一个域一定是一个欧氏环.

证 设 F 是域.

1) $\forall x(\neq 0)\in F,\phi:x\to n$(这里 n 是任意一个固定的非负整数)显然是集 $F-\{0\}$ 到非负整数集的一个映射.

2) 给定 $a(\neq 0)\in F$,因 F 是域,故 a 有逆元 $a^{-1}\in F$. $\forall b\in F$,有 $b=(ba^{-1})a+0$,这里 $ba^{-1},0\in F$.

所以 F 是一个欧氏环.

2. 我们看有理数域 $\mathbb{Q}$ 上的一元多项式环 $\mathbb{Q}[x]$. 理想 (x^2+1,x^5+x^3+1) 等于怎样的一个主理想?

解 已知 $\mathbb{Q}[x]$ 是欧氏环②.而且 $\mathbb{Q}[x]$ 是主理想环③.设 $(x^2+1,x^5+x^3+1)=(f(x))$. 由第十四章,二,7,$f(x)$ 是 x^2+1,x^5+x^3+1 的一个最大公因子.因 x^2+1,x^5+x^3+1 互素,故 $(x^2+1,x^5+x^3+1)=(1)=\mathbb{Q}[x]$.

3. 证明由所有复数 $a+bi(a,b$ 是整数)所作成的环是一个欧氏环(取 $\phi(\alpha)=|\alpha|^2$).

证一 $\mathbb{Z}[\mathrm{i}]=\left\{a+bi\,\middle|\,a,b\in\mathbb{Z}\right\}$ 是整环.

1) $\forall\alpha(\neq 0)\in\mathbb{Z}[\mathrm{i}],\phi:\alpha\to|\alpha|^2$ 显然是集 $\mathbb{Z}[\mathrm{i}]-\{0\}$ 到非负整数集的一个映射.

2) 给定 $\alpha=a+bi(\neq 0)\in\mathbb{Z}[\mathrm{i}]$,$\forall\beta\in\mathbb{Z}[\mathrm{i}]$,要找 $q,r\in\mathbb{Z}[\mathrm{i}]$,使得 $\beta=q\alpha+r$,$r=0$ 或 $\phi(r)<\phi(\alpha)$. 因 $\alpha=a+bi(\neq 0)\in\mathbb{Z}[\mathrm{i}]\subset\mathbb{C}$,故 $\exists\alpha^{-1}=\dfrac{a}{a^2+b^2}+\dfrac{-b}{a^2+b^2}\mathrm{i}\in\mathbb{C}$,使得 $\alpha^{-1}\alpha=1$,从而 $\beta=(\beta\alpha^{-1})\alpha$. 令 $h=\beta\alpha^{-1}=h_1+h_2\mathrm{i}$,其中 $h_1,h_2\in\mathbb{Q}$. 取

① 张禾瑞.近世代数基础.北京:高等教育出版社,1978.147.定理2.

② 同上.140.定理3.

③ 同上.139.定理1.

$$q_1=[h_1]\text{或}[h_1]+1,\ q_2=[h_2]\text{或}[h_2]+1,$$

其中$[h_i]$是不超过h_i的最大整数,即取q_i为最接近h_i的整数,$i=1,2$. 则有

$$|h_1-q_1|\leqslant\frac{1}{2},\ |h_2-q_2|\leqslant\frac{1}{2}.$$

令$q=q_1+q_2\mathrm{i}$,则$q\in\mathbb{Z}[\mathrm{i}]$且

$$\beta=(\beta\alpha^{-1})\alpha=h\alpha=q\alpha+(h\alpha-q\alpha)=q\alpha+(h-q)\alpha=q\alpha+r,$$

其中$r=(h-q)\alpha$. 因$h\alpha=(\beta\alpha^{-1})\alpha=\beta\in\mathbb{Z}[\mathrm{i}]$,$q\alpha\in\mathbb{Z}[\mathrm{i}]$,故$r\in\mathbb{Z}[\mathrm{i}]$. 于是$r=0$或

$$|r|^2=|(h-q)\alpha|^2=|h-q|^2|\alpha|^2=\left[(h_1-q_1)^2+(h_2-q_2)^2\right]|\alpha|^2$$
$$=[|h_1-q_1|^2+|h_2-q_2|^2]|\alpha|^2\leqslant\left(\frac{1}{4}+\frac{1}{4}\right)|\alpha|^2=\frac{1}{2}|\alpha|^2<|\alpha|^2,$$

即$\phi(r)<\phi(\alpha)$. 综上,$\mathbb{Z}[\mathrm{i}]$是一个欧氏环.

证二　$\mathbb{Z}[\mathrm{i}]=\left\{a+b\mathrm{i}\,\middle|\,a,b\in\mathbb{Z}\right\}$是整环.

1)　同证一.

2)　给定$\alpha=a+b\mathrm{i}(\neq0)\in\mathbb{Z}[\mathrm{i}]$,有$|\alpha|^2=a^2+b^2\neq0$. $\forall\beta=c+d\mathrm{i}\in\mathbb{Z}[\mathrm{i}]$,要证$\exists q=q_1+q_2\mathrm{i},r\in\mathbb{Z}[\mathrm{i}]$,使得$\beta=q\alpha+r$,其中$r=0$或$\phi(r)<\phi(\alpha)$,即$|r|^2<|\alpha|^2$,即$\frac{|r|^2}{|\alpha|^2}=\left|\frac{r}{\alpha}\right|^2<1$.

只需证$\beta-q\alpha=r$,$\left|\frac{\beta}{\alpha}-q\right|^2=\left|\frac{r}{\alpha}\right|^2<1$. 我们现在来证明这个式子.

$$\left|\frac{\beta}{\alpha}-q\right|^2=\left|\frac{c+d\mathrm{i}}{a+b\mathrm{i}}-(q_1+q_2\mathrm{i})\right|^2=\left|\left(\frac{ac+bd}{a^2+b^2}-q_1\right)+\left(\frac{ad-bc}{a^2+b^2}-q_2\right)\mathrm{i}\right|^2$$
$$=\left(\frac{ac+bd}{a^2+b^2}-q_1\right)^2+\left(\frac{ad-bc}{a^2+b^2}-q_2\right)^2=\left|\frac{ac+bd}{a^2+b^2}-q_1\right|^2+\left|\frac{ad-bc}{a^2+b^2}-q_2\right|^2.$$

因此,取

$$q_1=\left[\frac{ac+bd}{a^2+b^2}\right]\text{或}\left[\frac{ac+bd}{a^2+b^2}\right]+1,\ q_2=\left[\frac{ad-bc}{a^2+b^2}\right]\text{或}\left[\frac{ad-bc}{a^2+b^2}\right]+1.$$

(见证一)令$q=q_1+q_2\mathrm{i}\in\mathbb{Z}[\mathrm{i}]$,可使

$$\left|\frac{\beta}{\alpha}-q\right|^2\leqslant\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2=\frac{1}{2}<1.$$

令$r=\beta-q\alpha\in\mathbb{Z}[\mathrm{i}]$,有$\beta=q\alpha+r$且$r=0$或$\left|\frac{r}{\alpha}\right|^2=\left|\frac{\beta}{\alpha}-q\right|^2<1$,即$\frac{|r|^2}{|\alpha|^2}<1$,即$|r|^2<|\alpha|^2$,从而$\phi(r)<\phi(\alpha)$. 所以$\mathbb{Z}[\mathrm{i}]$是一个欧氏环.

4. 假定I是一个唯一分解环,Q是I的商域. 证明:$I[x]$的一个多项式若是在$Q[x]$里可约,则它在$I[x]$里已经可约.

证一　设$f(x)(\in I[x])$在$Q[x]$里可约,显然$f(x)\neq0$,又因I是唯一分解环,故由第十五章,一,6,3),$f(x)=df_0(x)$,其中$d(\in I)$是$f(x)$的系数的最大公因子,$f_0(x)$在$I[x]$里本原. 因$d\neq0$,故d是域Q的单位,从而$f(x)$,$f_0(x)$在$Q[x]$中相伴. 因$f(x)$在$Q[x]$里可约,故由第十四章,一,5,$f_0(x)$在$Q[x]$里也可约. 由第十五章,一,7,$f_0(x)$在$I[x]$里可约. 由第十五章,一,4,$f_0(x)=g_1(x)g_2(x)$,其中$g_i(x)\in I[x]$,$0<\deg g_i(x)<\deg f(x)$,$i=1,2$. 于是$f(x)=dg_1(x)g_2(x)$,其中$dg_1(x)$,$g_2(x)$都不是$I[x]$的单位. 因此$f(x)$在$I[x]$里有真因子. 所以$f(x)$在$I[x]$里可约.

证二 设 $f(x)(\in I[x])$ 在 $Q[x]$ 里可约，由证一，$f(x)=df_0(x)$，其中 $d\in I$，$f_0(x)$ 在 $I[x]$ 里本原．由第十五章，一，4，注 3)，$f(x)=g(x)h(x)$，其中 $g(x),h(x)\in Q[x]$，$0<\deg g(x)<\deg f(x)$，$0<\deg h(x)<\deg f(x)$．由第十五章，一，6，$g(x)=\frac{b}{a}g_0(x)$，$h(x)=\frac{l}{c}h_0(x)$，其中 $a,b,c,l\in I$，$g_0(x)$，$h_0(x)$ 都在 $I[x]$ 里本原．从而 $f(x)=\frac{bl}{ac}g_0(x)h_0(x)$．由第十五章，一，5，$g_0(x)h_0(x)$ 在 $I[x]$ 里本原．由第十五章，一，6，$f_0(x)=\varepsilon g_0(x)h_0(x)$，其中 ε 是 I 的单位．于是 $f(x)=d\varepsilon g_0(x)h_0(x)$．因 $\deg \varepsilon g_0(x)=\deg g(x)>0$，故 $\varepsilon g_0(x)\overline{\in} I$，从而 $\varepsilon g_0(x)$ 不是 $I[x]$ 的单位．同理 $h_0(x)$ 也不是 $I[x]$ 的单位．因此 $f(x)$ 在 $I[x]$ 里有真因子．所以 $f(x)$ 在 $I[x]$ 里可约．

证三 设 $f(x)(\in I[x])$ 在 $Q[x]$ 里可约，显然 $f(x)\neq 0$，$f(x)$ 不是 $Q[x]$ 的单位，即 $f(x)$ 不是 Q 的单位，从而 $\deg f(x)>0$.

若 $f(x)$ 在 $I[x]$ 里本原，则由第十五章，一，7，$f(x)$ 在 $I[x]$ 里可约．

若 $f(x)$ 在 $I[x]$ 里非本原，则 $f(x)$ 的系数的最大公因子 $d(\in I)$ 不是 $I[x]$ 的单位．因 $d\neq 0$，故 $\deg d=0$，但 $\deg f(x)>0$，从而 d 不是 $f(x)$ 的相伴元．今 $d\mid f(x)$，因此 d 是 $f(x)$ 在 $I[x]$ 里的真因子．所以 $f(x)$ 在 $I[x]$ 里可约．

注 1) 证一的主要思路：$f(x)$ 在 $Q[x]$ 里可约 $\Rightarrow f(x)=df_0(x)$ 中 $f_0(x)$ 在 $Q[x]$ 里可约，在 $I[x]$ 里本原 $\Rightarrow f_0(x)$ 在 $I[x]$ 里可约 $\Rightarrow f(x)=df_0(x)$ 在 $I[x]$ 里可约．

2) 证二的主要思路：$f(x)$ 在 $Q[x]$ 里可约 $\Rightarrow f(x)=df_0(x)$，$f(x)=g(x)h(x)=\frac{bl}{ac}g_0(x)h_0(x)$，$f_0(x)$，$g_0(x)$，$h_0(x)$ 都在 $I[x]$ 里本原 $\Rightarrow f_0(x)=\varepsilon g_0(x)h_0(x)$，$\varepsilon$ 是 I 的单位 $\Rightarrow f(x)=d\varepsilon g_0(x)h_0(x)$ 在 $I[x]$ 里可约．

3) 该命题的逆否命题是：设 Q 是唯一分解环 I 的商域．若 $f(x)$ 在 $I[x]$ 里不可约，则 $f(x)$ 在 $Q[x]$ 里也不可约．

4) 因有理数域 $\mathbb{Q}$ 是整数环 $\mathbb{Z}$ 的商域，故：若 $f(x)(\in\mathbb{Z}[x])$ 在 $\mathbb{Z}$ 上不可约，则 $f(x)$ 在 $\mathbb{Q}$ 上也不可约．所以讨论整系数多项式在 $\mathbb{Q}$ 上是否不可约，可在 $\mathbb{Z}$ 上来考虑．

5. 假定 $I[x]$ 是整环 I 上的一元多项式环．$f(x)$ 属于 $I[x]$ 但不属于 I，并且 $f(x)$ 的最高系数是 I 的一个单位．证明：$f(x)$ 在 $I[x]$ 里有分解．

证一 若 $f(x)$ 是 $I[x]$ 的一个不可约多项式，则 $f(x)$ 已有分解．

若 $f(x)$ 在 I 上不是不可约，因 $f(x)\overline{\in} I$，故 $f(x)\neq 0$，$f(x)\neq I[x]$ 的单位，于是 $f(x)$ 在 I 上可约．从而 $f(x)$ 有真因子 $g(x)\in I[x]$，使得 $f(x)=g(x)h(x)$．且 $h(x)(\in I[x])$ 也是 $f(x)$ 的真因子．显然 $g(x)\neq 0$，$h(x)\neq 0$．下面证明 $\deg g(x)>0$．事实上，若 $\deg g(x)=0$，则 $g(x)=a\in I$，即 $f(x)=ah(x)$．因 $f(x)$ 的最高系数是 I 的一个单位 ε，故 $a\mid\varepsilon$，由第十四章，一，2，3)，$a=g(x)$ 是 I 的单位，此与 $g(x)$ 是 $f(x)$ 的真因子矛盾．所以 $\deg g(x)>0$，同理 $\deg h(x)>0$．因此 $\deg g(x)<\deg f(x)$，$\deg h(x)<\deg f(x)$．因 $f(x)$ 的最高系数是 I 的一个单位，故 $g(x)$ 和 $h(x)$ 的最高系数都是 I 的单位，且 $g(x)$，$h(x)$ 都不属于 I．于是可以对 $g(x)$ 和 $h(x)$ 进行类似于对 $f(x)$ 的讨论．由于 $f(x)$ 的次数是有限正整数，因此经有限步骤后，必可在 $I[x]$ 里将 $f(x)$ 分解成有限个不可约多项式的乘积．

证二 因 $f(x)\overline{\in} I$，故 $\deg f(x)=n>0$．现对 n 作数学归纳法．

$n=1$ 时，$f(x)$不可约，命题显然成立．

假定 $\deg s(x)<n$，且 $s(x)\in I[x]$，$s(x)\overline{\in} I$，$s(x)$的最高系数是 I 的一个单位时，命题成立．今看 $\deg f(x)=n$ 时：若 $f(x)$不可约，则命题已成立．若 $f(x)$不是不可约，由 $f(x)\overline{\in} I$，则 $f(x)$可约，从而 $f(x)=g(x)h(x)$. 由 $f(x)$的最高系数是单位知，$g(x)$，$h(x)$的最高系数也都是单位且 $\deg g(x)>0$，$\deg h(x)>0$（见证一），即 $g(x)$，$h(x)\overline{\in} I$. 于是 $\deg g(x)<\deg f(x)=n$，$\deg h(x)<\deg f(x)=n$. 由归纳假定，$g(x)$，$h(x)$都有分解，所以 $f(x)$也有分解.

依归纳原理，命题得证．

注　1)　证明的关键步骤是利用条件：$f(x)$的最高系数是单位，才能保证 $f(x)=g(x)h(x)$中的 $\deg g(x)>0$，$\deg h(x)>0$，也才能保证 $\deg g(x)<\deg f(x)$，$\deg h(x)<\deg f(x)$.

2)　该题中的 I 是整环，未必是唯一分解环，从而证明中不要使用本原多项式概念．

6. 假定 $\mathbb{Z}_{16}$是模 16 的剩余类环．$\mathbb{Z}_{16}[x]$的多项式 x^2 在 $\mathbb{Z}_{16}$里有多少个根？

解一　首先给出定义：设 R 是有单位元的交换环，$f(x)\in R[x]$. 若 $c\in R$，使 $f(c)=0$，则称 c 是 $f(x)$的一个根．

设 $f(x)=x^2$. 因 $f([0])=[0]$，$f([4])=[0]$，$f([8])=[0]$，$f([12])=[0]$，而 $\mathbb{Z}_{16}$中其余的元$[a]$都不能使 $f([a])=[0]$，故 $f(x)$在 $\mathbb{Z}_{16}$里有且只有 4 个根：$[0]$，$[4]$，$[8]$，$[12]$.

解二　$[m](\in\mathbb{Z}_{16})$是$f(x)=x^2$的根$\Leftrightarrow[m^2]=[0]\Leftrightarrow[m]^2=[0]\Leftrightarrow 16\,\big|\,m^2$. 在$0,1,2,\cdots,15$的 16 个数中，有且只有 4 个数：0，4，8，12 其平方被 16 整除．所以 $f(x)$的根是$[0]$，$[4]$，$[8]$，$[12]$.

注　$f(x)=x^2\in\mathbb{Z}_{16}[x]$是二次多项式，却有 $4(>\deg x^2=2)$个根，因为 $\mathbb{Z}_{16}$不是整环．

例　$\mathbb{Z}_6$里全部 6 个元都是 x^3-x 的根．$x^2-[4]$在 $\mathbb{Z}_{12}$里有 4 个根：$[2]$，$[4]$，$[8]$，$[10]$.

7. 假定 $\mathbb{Z}_3$是模 3 的剩余类环，我们看 $\mathbb{Z}_3[x]$的多项式 $f(x)=x^3-x$. 证明：$f(\alpha)=0$，不管 α 是 $\mathbb{Z}_3$的哪一个元．

证一　因 $f(x)=x^3-x=x(x^2-1)=x(x-1)(x+1)=x(x-1)(x-[2])$，故 $f([0])=f([1])=f([2])=[0]$.

证二　$\forall\alpha\in\mathbb{Z}_3$，$\alpha^3=\alpha$，从而 $f(\alpha)=\alpha^3-\alpha=0$.

8. 证明本节的导数计算规则：

$$[f(x)+g(x)]'=f'(x)+g'(x).$$

$$[f(x)g(x)]'=f(x)g'(x)+g(x)f'(x).$$

$$[f(x)^t]'=tf(x)^{t-1}f'(x).$$

证　设 $f(x)=\sum\limits_{i=0}^{n}a_ix^i$，$g(x)=\sum\limits_{i=0}^{n}b_ix^i\in I[x]$（缺项补零）.

1)　$[f(x)+g(x)]'=\left[\sum\limits_{i=0}^{n}(a_i+b_i)x^i\right]'=\sum\limits_{i=1}^{n}i(a_i+b_i)x^{i-1}=\sum\limits_{i=1}^{n}ia_ix^{i-1}+\sum\limits_{i=1}^{n}ib_ix^{i-1}=f'(x)+g'(x)$.

2)　$[f(x)g(x)]'=\left[\sum\limits_{k=0}^{2n}\left(\sum\limits_{i+j=k}a_ib_jx^k\right)\right]'=\sum\limits_{k=1}^{2n}\sum\limits_{i+j=k}ka_ib_jx^{k-1}=\sum\limits_{k=1}^{2n}\sum\limits_{i+j=k}(i+j)a_ib_jx^{k-1}=$

$\sum\limits_{k=1}^{2n}\sum\limits_{i+j=k}a_i(jb_j)x^{k-1}+\sum\limits_{k=1}^{2n}\sum\limits_{i+j=k}(ia_i)b_jx^{k-1}=\left(\sum\limits_{i=0}^{n}a_ix^i\right)\left(\sum\limits_{j=1}^{n}jb_jx^{j-1}\right)+\left(\sum\limits_{j=0}^{n}b_jx^j\right)\left(\sum\limits_{i=1}^{n}ia_ix^{i-1}\right)=$

$f(x)g'(x)+g(x)f'(x)$.

3) 对 t 作数学归纳法.

$t=2$ 时,利用本题 2),有

$$\left[f(x)^2\right]'=f(x)f'(x)+f(x)f'(x)=2f(x)^{2-1}f'(x).$$

假设 $t=k$ 时,$\left[f(x)^k\right]'=kf(x)^{k-1}f'(x)$. 今看 $t=k+1$ 时,$\left[f(x)^{k+1}\right]'=\left[f(x)f(x)^k\right]'=f(x)\left[f(x)^k\right]'+f(x)^kf'(x)\underset{\text{假设}}{\overset{\text{归纳}}{=\!=}}f(x)\left[kf(x)^{k-1}f'(x)\right]+f(x)^kf'(x)=(k+1)f(x)^kf'(x)$.

所以,$\left[f(x)^t\right]'=tf(x)^{t-1}f'(x)$.

注 1) $\left[cf(x)\right]'=cf'(x),c\in I$.

2) $\left[af(x)+bg(x)\right]'=af'(x)+bg'(x),a,b\in I$.

3) $\left[f_1(x)+f_2(x)+\cdots+f_s(x)\right]'=f_1'(x)+f_2'(x)+\cdots+f_s'(x)$.

4) $\left[f_1(x)f_2(x)\cdots f_s(x)\right]'=f_1'(x)f_2(x)\cdots f_s(x)+f_1(x)f_2'(x)\cdots f_s(x)+\cdots+f_1(x)f_2(x)\cdots f_s'(x)$.

5) 在数学分析中,若 $f'(x)=0$,则 $f(x)$是一个常量. 但在整环上,此结论未必成立. 例,设 $f(x)=x^2\in\mathbb{Z}_2[x]$,则 $f'(x)=[2]x=[0]x=[0]$. 但 $f(x)=x^2\overline{\in}\mathbb{Z}_2$.

我们这里 $f(x)$的导数 $f'(x)$是形式地定义,与极限、连续概念无关.

三、讲与练

1. 判断下面各命题是否正确.

1) 欧氏环的子环是欧氏环.

2) 设 Q 是整环 I 的商域,则 Q 的单位是 I 的单位.

3) 设 F 是域,则

$$f(x)\text{是 }F[x]\text{的单位}\Leftrightarrow f(x)\text{是域 }F\text{ 中的非零元}.$$

4) 设 F 是域,则 $f(x)\,(\in F[x])$的所有相伴元是 $cf(x)$,其中 c 是 $F[x]$中的零次多项式.

5) 在 $\mathbb{Z}[x]$中,

$$f(x)\text{ 与 }g(x)\text{ 相伴}\Leftrightarrow f(x)=g(x)\text{ 或 }-g(x).$$

6) $[1](x^2+1)$与$[2](x^2+1)$是 x^2+1 在 $\mathbb{Z}_3[x]$中的全部相伴元.

7) 与本原多项式相伴的多项式也是本原多项式.

8) 设 I 是唯一分解环,若 $f(x)\,(\in I[x])$的某个系数为单位,则 $f(x)$本原.

9) 设 I 是唯一分解环,若 $f(x)\,(\in I[x])$的最高系数是单位元,则 $f(x)$本原.

10) 域 F 上的非零多项式都是 $F[x]$的本原多项式.

11) 设 I 是唯一分解环,若 $f(x)(\neq 0)\in I$,则

$$f(x)\text{ 是 }I[x]\text{ 的本原多项式}\Leftrightarrow f(x)\text{ 是单位}.$$

12) 设 I 是整环, $f(x)\in I[x]$,则

$$f(x)\text{ 不可约}\Leftrightarrow f(x)\text{ 没有分解}.$$

13）设 I 是整环，$ax+b\in I[x]$，$a\neq 0$，则

$$a \text{ 是 } I \text{ 的单位} \Rightarrow ax+b \text{ 在 } I[x] \text{ 中不可约}.$$

14）设 $f(x),g(x)\in\mathbb{Z}[x]$. 若 $f(x),g(x)$ 在 $\mathbb{Q}$ 上互素，则 $f(x),g(x)$ 在 $\mathbb{Z}_p$ 上互素，其中 p 是素数.

15）$\mathbb{Z}/(p)[x]$ 是一个唯一分解环，其中 p 是素数.

16）设 I 是唯一分解环，$f(x)(\neq 0),g(x)\in I[x]$，$f(x)=af_0(x)$，$g(x)=bg_0(x)$，其中 $a,b\in I$，$f_0(x),g_0(x)$ 本原. 若 $g(x)\mid f(x)$，则 $b\mid a$，$g_0(x)\mid f_0(x)$.

17）设 I 是整环，$f(x)\in I[x]$. 若 $x-\alpha\mid f'(x)$，则 α 是 $f(x)$ 的重根.

18）设 I 是整环，$f(x)\in I[x]$，$\alpha\in I$，则

$$\alpha \text{ 是 } f(x) \text{ 的重根} \Leftrightarrow x-\alpha \text{ 是 } f(x) \text{ 与 } f'(x) \text{ 的公因子}.$$

19）设 $I[x]$ 是整环，$f(x)\in I[x]$，$\alpha\in I$，则

$$\alpha \text{ 是 } f(x) \text{ 的重根} \Leftrightarrow x-\alpha\mid d(x),\ d(x) \text{ 是 } f(x),\ f'(x) \text{ 的一个最大公因子}.$$

解　1）不正确. 例，欧氏环 $\mathbb{Q}[x]$ 的子环 $\mathbb{Z}[x]$ 不是欧氏环，因 $\mathbb{Z}[x]$ 不是主理想环.

2）不正确. 例，$\mathbb{Q}$ 是 $\mathbb{Z}$ 的商域，2 是 $\mathbb{Q}$ 的单位，但 2 不是 $\mathbb{Z}$ 的单位.

3）正确. 事实上，设 F 是域，则

$f(x)$ 是 $F[x]$ 的单位 $\Leftrightarrow f(x)$ 是 F 的单位 $\Leftrightarrow f(x)$ 是 F 中的非零元. 见第十一章，四，1，11).

4）正确. 因为 $F[x]$ 中的所有零次多项式就是 $F[x]$ 的所有单位.

5）正确. 因为 $\mathbb{Z}[x]$ 的单位有且只有 ± 1.

6）正确. 因为 $[1]$，$[2]$ 是 $\mathbb{Z}_3[x]$ 的全部单位.

7）正确. 直接由本原多项式定义可知.

8）正确. 由定义可知.

9）正确. 由定义可知.

10）正确. 因为域 F 中的非零元都是 F 的单位.

11）正确. 利用本原多项式定义易证.

12）不正确. 若 $f(x)$ 不可约，则 $f(x)=f(x)$ 已经有分解. 反之，若 $f(x)$ 没有分解，但 $f(x)$ 未必不可约. 例，$I=\left\{a_1x^{\alpha_1}+a_2x^{\alpha_2}+\cdots+a_nx^{\alpha_n}\,\middle|\, a_i\in \text{域 } F, \alpha_i \text{ 是非负有理数}, n \text{ 是正整数}\right\}$ 是整环. x 在 I 里没有分解. 但 $x\neq 0$，$x\neq I[x]$ 的单位，x 在 $I[x]$ 里有真因子 $x^{\frac{1}{2}}$，从而 x 在 $I[x]$ 里可约（见第十四章，四，3）.

13）正确. 事实上，当 a 是 I 的单位时，$ax+b\neq 0$，$\neq I[x]$ 的单位，且 $ax+b$ 的因子只有 $I[x]$ 的单位或本身的相伴元.

注　① 当 a 不是 I 的单位时，一次多项式 $ax+b$ 有可能是 I 上的可约多项式或不可约多项式. 例，一次多项式 $5x+5=5(x+1)$ 在 $\mathbb{Z}[x]$ 中可约，而在 $\mathbb{Q}[x]$ 中不可约. $5x+1$ 在 $\mathbb{Z}[x]$ 中不可约，其中 5 不是 $\mathbb{Z}$ 的单位.

② 域 F 上每个一次多项式都是不可约的.

14）不正确. 例，设 $f(x)=x$，$g(x)=x+p\in\mathbb{Z}[x]$，其中 p 是素数，则 $f(x),g(x)$ 在 $\mathbb{Q}[x]$ 上互素. 但在 $\mathbb{Z}_p$ 上，$f(x)=g(x)=x$，因此 $f(x),g(x)$ 在 $\mathbb{Z}_p$ 上不互素.

15）正确. 因 $\mathbb{Z}/(p)$（p 是素数）是域，故是唯一分解环，从而 $\mathbb{Z}/(p)[x]$ 也是唯一分解环.

16） 正确．事实上，因 $g(x) \mid f(x)$，即 $bg_0(x) \mid af_0(x)$，故 $\exists h(x) \in I[x]$，使得 $af_0(x) = bg_0(x)h(x)$．设 $h(x) = ch_0(x)$，其中 $c \in I$，$h_0(x)$本原，则 $f(x) = af_0(x) = bcg_0(x)h_0(x)$．由第十五章，一，5，$g_0(x)h_0(x)$本原．从而 a 与 bc 都是 $f(x)$的系数的最大公因子，因此 $bc = a\varepsilon$，ε 是单位．于是 $af_0(x) = a\varepsilon g_0(x)h_0(x)$．因 $f(x) \neq 0$，故 $a \neq 0$，由消去律，$f_0(x) = \varepsilon g_0(x)h_0(x)$．所以 $g_0(x) \mid f_0(x)$．由 $a = bc\varepsilon^{-1}$，有 $b \mid a$．

请读者考虑，$f(x) = 0$ 时，命题是否仍成立．

17） 不正确．例，设 $f(x) = \frac{1}{2}x^2 - x \in \mathbb{Q}[x]$，则 $f'(x) = x - 1$，$x - 1 \mid f'(x)$．但 1 不是$f(x)$的重根．

18） 正确[①]．

19） 不正确．因为 $f(x)$，$f'(x)$的最大公因子在整环 $I[x]$里未必存在．

2.（余式定理）设 I 是整环，$f(x)$，$x - c \in I[x]$．证明，$x - c$ 除 $f(x)$所得的余式为 $f(c)$．

证 由第十五章，一，2，$\exists q(x)$，$r(x) \in I[x]$，使得 $f(x) = q(x)(x - c) + r(x)$，其中余式 $r(x) = 0$ 或 $\deg r(x) < \deg(x - c) = 1$，因此，$r(x) = r \in I$．从而 $f(c) = q(c)(c - c) + r$．所以余式 $r = f(c)$．

注 可推广为下面命题：设 I 是整环，$f(x)$，$bx + c \in I[x]$，其中 b 是 I 的单位．证明：$bx + c$除 $f(x)$所得的余式为 $f(-b^{-1}c)$．

事实上，$f(x) = q(x)(bx + c) + r$，$q(x) \in I[x]$，$r \in I$．
从而 $f(-b^{-1}c) = q(-b^{-1}c)[b(-b^{-1}c) + c] + r = r$．

3. 设 F 是域，$f(x) \in F[x]$，$\deg f(x) = 2$ 或 3．证明：

$$f(x)\text{在 } F[x]\text{中可约} \Leftrightarrow f(x)\text{在 } F \text{ 中有根}．$$

证 （$\Rightarrow$） 若 $f(x)$在 $F[x]$中可约，则由第十五章，一，4，注 3），$f(x) = g(x)h(x)$，其中 $g(x)$，$h(x) \in F[x]$，$0 < \deg g(x) < \deg f(x)$，$0 < \deg h(x) < \deg f(x)$．今 $\deg f(x) = 2$ 或 3，又 $\deg f(x) = \deg g(x) + \deg h(x)$，从而 $g(x)$与 $h(x)$中必有一个是一次的．不妨设 $g(x) = ax + b$，其中 $a \neq 0$．因 F 是域，故 $\exists a^{-1} \in F$．于是由 $g(x) = a(x + a^{-1}b)$，a 是$F[x]$的单位，$x + a^{-1}b \mid f(x)$．所以$-a^{-1}b(\in F)$是 $f(x)$的一个根[②]．

（$\Leftarrow$） 若 $f(x)$在 F 中有根 α，则 $x - \alpha \mid f(x)$[③]．因 $\deg f(x) = 2$ 或 3，故 $x - \alpha$ 是 $f(x)$ 的真因子．又 $f(x) \neq 0$，$f(x) \neq$ 单位，从而 $f(x)$在 $F[x]$中可约．

注 该命题的逆否命题是：设 F 是域，$f(x) \in F[x]$，$\deg f(x) = 2$ 或 3．则

$$f(x)\text{在 } F[x]\text{中不可约} \Leftrightarrow f(x)\text{在 } F \text{ 中没有根}．$$

4. 判断下列各多项式 $f(x)$在 $I[x]$中的可约性．

1） $f(x) = x^2 + 1$．$I = \mathbb{Z}_3$．

2） $f(x) = x^2 - [2]$．$I = \mathbb{Z}_7$．

3） $f(x) = x^2 + [3]$．$I = \mathbb{Z}_5$．

---

① 张禾瑞．近世代数基础．北京：高等教育出版社，1978．150．定理 3．

②③ 同上．148．定理 1．

4)　$f(x)=x^2+4$. $I=\mathbb{Q}$.

5)　$f(x)=x^2+[2]x$. $I=\mathbb{Z}_3$.

6)　$f(x)=x^2+x+1$. $I=\mathbb{Z}_2$.

7)　$f(x)=x^3-x$. $I=\mathbb{Z}_3$.

8)　$f(x)=x^3+x+1$. $I=\mathbb{Z}_5$.

9)　$f(x)=x^3+x^2+1$. $I=\mathbb{Z}_2$.

10)　$f(x)=x^3+x^2+[2]$. $I=\mathbb{Z}_3$.

11)　$f(x)=x^5-1$. $I=\mathbb{Z}_5$.

12)　$f(x)=x^5+[3]x^3+x^2+[2]x$. $I=\mathbb{Z}_5$.

解　1)　利用上面3题来判断．因 x^2+1 在 $\mathbb{Z}_3$ 中无根，故 x^2+1 在 $\mathbb{Z}_3[x]$ 中不可约．而 x^2+1 在 $\mathbb{Z}_5$ 中有根[2]，从而 x^2+1 在 $\mathbb{Z}_5[x]$ 中可约．

2)　$x^2-[2]$ 在 $\mathbb{Z}_7$ 中有根[3]，从而在 $\mathbb{Z}_7[x]$ 中可约．

3)　$x^2+[3]$ 在 $\mathbb{Z}_5$ 中无根，从而在 $\mathbb{Z}_5[x]$ 中不可约．

4)　x^2+4 在 $\mathbb{Q}$ 中无根，从而在 $\mathbb{Q}[x]$ 中不可约．而 x^2+4 在 $\mathbb{Z}_5$ 中有根[1]，从而在 $\mathbb{Z}_5[x]$ 中可约．

5)　$x^2+[2]x$ 在 $\mathbb{Z}_3$ 中有根[1]，从而在 $\mathbb{Z}_3[x]$ 中可约．

6)　$\mathbb{Z}_2$ 中的元都不是 x^2+x+1 的根，从而 x^2+x+1 在 $\mathbb{Z}_2[x]$ 中不可约．但 x^2+x+1 在 $\mathbb{Z}_7[x]$ 中可约，因在 $\mathbb{Z}_7$ 中有根[2].

7)　x^3-x 在 $\mathbb{Z}_3[x]$ 中可约，因在 $\mathbb{Z}_3$ 中有根[0].

8)　x^3+x+1 在 $\mathbb{Z}_5[x]$ 中不可约，因在 $\mathbb{Z}_5$ 中无根．但 x^3+x+1 在 $\mathbb{Z}_3$ 中有根[1]，从而在 $\mathbb{Z}_3$ 上可约．

9)　x^3+x^2+1 在 $\mathbb{Z}_2$ 中无根，从而在 $\mathbb{Z}_2[x]$ 中不可约．

10)　$x^3+x^2+[2]$ 在 $\mathbb{Z}_3[x]$ 中不可约，因在 $\mathbb{Z}_3$ 中无根．

11)　x^5-1 在 $\mathbb{Z}_5$ 中有根[1]，从而在 $\mathbb{Z}_5[x]$ 中可约．

12)　显然[0]是 $x^5+[3]x^3+x^2+[2]x$ 在 $\mathbb{Z}_5$ 中的根，从而这个多项式在 $\mathbb{Z}_5[x]$ 中可约．

5. 将下列各多项式 $f(x)$ 在 $I[x]$ 中分解为不可约多项式的积．

1)　$f(x)=4x^2-4x+8$. $I=\mathbb{Z}$.

2)　$f(x)=x^3+[2]x^2+[2]x+[4]$. $I=\mathbb{Z}_7$.

3)　$f(x)=x^4+1$. $I=\mathbb{Z}_5$.

4)　$f(x)=x^4+[3]x^3+[2]x+[4]$. $I=\mathbb{Z}_5$.

解　1)　$4x^2-4x+8=2\cdot 2(x^2-x+2)$，其中 $2, x^2-x+2$ 都在 $\mathbb{Z}$ 上不可约．

2)　因[5]是 $f(x)$ 的一个根，故 $f(x)=(x-[5])(x^2+[2])$，其中 $x-[5], x^2+[2]$ 都在 $\mathbb{Z}_7$ 上不可约．

3)　$x^4+1=(x^2+[2])(x^2+[3])$，其中 $x^2+[2], x^2+[3]$ 都在 $\mathbb{Z}_5$ 上不可约，因为 $\mathbb{Z}_5$ 的所有元都不是它们的根．

4)　因[1]与[4]都是 $f(x)$ 的根，故 $f(x)=(x-1)^3(x-[4])$，其中 $x-1, x-[4]$ 都在 $\mathbb{Z}_5$ 上不可约．

四、思考问题

1. 证明：整环 $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$ 是一个欧氏环．

2. 证明：$I=\left\{a+b\sqrt{3}\,\mathrm{i}\,\middle|\, a,b\right.$ 或都是整数，或都是奇数的 $\left.\frac{1}{2}\right\}$ 是一个欧氏环．

3. 设 I 是欧氏环．又设从集 $I^*=I-\{0\}$ 到非负整数集的映射 ϕ 适合条件：$0\overline{\in}\phi(I^*)$，且 $\phi(ab)=\phi(a)\phi(b)$，$\forall a,b\in I^*$．证明：若 $a\in I$，则

$$a \text{ 是单位} \Leftrightarrow \phi(a)=1.$$

4. 设 $f(x)=x^3+x^2+x+1$，$g(x)=x^2+[3]x+[2]$.

1） 若 $f(x),g(x)\in\mathbb{Z}_5[x]$，$g(x)$ 能否整除 $f(x)$？

2） 若 $f(x),g(x)\in\mathbb{Z}_7[x]$，$g(x)$ 能否整除 $f(x)$？

5. 设 I 是唯一分解环，$f_1(x),f_2(x),\cdots$ 是 I 上本原多项式序列，且 $f_{i+1}(x)\mid f_i(x)$，$i=1,2,\cdots$. 证明：这个序列只含有限个互不相伴的多项式．

6. 1） $\mathbb{Q}[x]/(x^2+2)$ 中的元 $[x]$ 是否可逆元？若是，求出 $[x]$ 的逆元．

2） $\mathbb{Z}_3[x]/(x^2+1)$ 中的元 $\big[[2]x+[2]\big]$ 是否可逆元？若是，求出 $\big[[2]x+[2]\big]$ 的逆元．

7. 设 I 是整环，证明：在 $I[x]$ 中，

$$a_0+a_1x+\cdots+a_nx^n \text{ 不可约} \Leftrightarrow a_n+a_{n-1}x+\cdots+a_0x^n \text{ 不可约}.$$

8. 设 I 是整环，$f(x),g(x)\in I[x]$，$\deg f(x)<n$，$\deg g(x)<n$. 若 $\exists\, a_1,a_2,\cdots,a_n\in I$ 且 $a_i\neq a_j\,(i\neq j)$，使得 $f(a_i)=g(a_i)$，$i=1,2,\cdots,n$，证明：$f(x)=g(x)$.

9. 设 I 是唯一分解环，$f(x)\in I[x]$，$f(x)$ 的最高系数为 1，Q 是 I 的商域．$\forall g(x)\in Q[x]$，$g(x)$ 的最高系数为 1 且 $g(x)\mid f(x)$. 证明：$g(x)\in I[x]$.

10. 设 $f(x)\in\mathbb{Z}[x]$，它的最高系数为 1，且 α 是它的任一有理根．证明：α 是整数．

11. 首先给出定义：设 R 是有单位元的交换环（可能有零因子），若 $\varepsilon(\in R)$ 有逆元，则称 ε 是 R 的单位．

设 R 是有单位元的交换环．$f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$，证明：

$f(x)$ 是 $R[x]$ 的单位 $\Leftrightarrow a_0$ 是 R 的单位，$a_1,a_2,\cdots,a_n$ 是 R 的幂零元（第九章，四，12）.

12. 证明：二次多项式 x^2+1 在四元数除环里有无限多个根．

13. 证明艾森斯坦因(Eisenstein)不可约性判别准则：设 I 是唯一分解环，$f(x)=a_0+a_1x+\cdots+a_nx^n\in I[x]$. 若 $\exists$ 素元 $p\in I$，使得 $p\nmid a_n$，$p\mid a_0$，$p\mid a_1$，$\cdots$，$p\mid a_{n-1}$，$p^2\nmid a_0$，则 $f(x)$ 或在 I 中有真因子，或在 $I[x]$ 中不可约．从而 $f(x)$ 在 $Q[x]$ 中也不可约，其中 Q 是 I 的商域（见第十五章，二，4，注 3））.

14. 证明：割圆多项式 $f(x)=x^{p-1}+x^{p-2}+\cdots+1$ 在 $\mathbb{Z}[x]$ 里不可约，其中 p 是素数．

15. 设 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0\in\mathbb{Z}[x]$，$\bar{f}(x)=[1]x^n+[a_{n-1}]x^{n-1}+\cdots+[a_0]\in\mathbb{Z}_p[x]$，$p$ 是素数．若 $\bar{f}(x)$ 在 $\mathbb{Z}_p$ 上不可约，证明：$f(x)$ 在 $\mathbb{Z}$ 上也不可约．

第十六章　扩域、素域、单扩域、代数扩域

一、基本问题问答

1. 关于命题：设 E 是域.

(i)　若 ch $E=\infty$，则 $\exists E$ 的一个（素）子域 F'，使得 $F'\cong$ 有理数域 $\mathbb{Q}$.

(ii)　若 ch $E=$ 素数 p，则 $\exists E$ 的一个（素）子域 R'，使得 $R'\cong \mathbb{Z}/(p)$，其中 $\mathbb{Z}$ 是整数环①.

1）　设 e 是 E 的单位元，$R'=\{ne \mid n\in\mathbb{Z}\}$ 为何是 E 的子域？

2）　ch $E=\infty$ 用在情形(i)的证明中的哪一步？

3）　ch $E=$ 素数 p 用在情形(ii)的证明中的哪一步？

4）　该命题的逆命题成立吗？

5）　$\mathbb{Q}$ 和 $\mathbb{Z}/(p)$（p 是素数）为何都不含真子域？

答　1）　见第十一章，三，10.

2）　ch $E=\infty$ 保证了映射 $\phi: n\to ne$ 是 $\mathbb{Z}$ 到 R' 的单射. 这是因为，$\forall n,m\in\mathbb{Z}$，若 $ne=me$，则 $(n-m)e=0$. 因 ch $E=\infty$，故 $n-m=0$，从而 $n=m$，所以 ϕ 是单射.

3）　因 ch $E=$ 素数 p，故 $\phi(p)=pe=0$，从而有 $p\in\ker\phi$，才有 $(p)\subset\ker\phi=\mathfrak{A}$.

4）　成立. 事实上，设 E 是域. (i)　若 $\exists E$ 的一个（素）子域 F'，使得 $F'\cong\mathbb{Q}$，则必 ch $E=\infty$. 这是因为，由第十一章，三，9，ch $E=$ ch $F'=$ ch $\mathbb{Q}=\infty$. (ii)　若 $\exists E$ 的一个（素）子域 R'，使得 $R'\cong\mathbb{Z}/(p)$，p 是素数，同样，由第十一章，三，9，ch $E=$ ch $R'=$ ch $\mathbb{Z}/(p)=p$.

5）　由《高等代数》②已知 $\mathbb{Q}$ 是最小数域，从而 $\mathbb{Q}$ 不含真子域. 设 H 是 $\mathbb{Z}/(p)$ 的任一子域，则 $\exists$ 单位元 $[1]\in H$. $\forall [n]\in\mathbb{Z}/(p)$，有 $[n]=n[1]\in H$，从而 $\mathbb{Z}/(p)\subset H$. 于是 $H=\mathbb{Z}/(p)$. 所以 $\mathbb{Z}/(p)$ 不含真子域. 即 $\mathbb{Q}$ 和 $\mathbb{Z}/(p)=\mathbb{Z}_p$ 都是素域.

注　1）　由该命题知，在同构意义下，素域 Δ 有且只有两种类型：ch$\Delta=\infty$ 时，$\Delta\cong\mathbb{Q}$（含无限多个元）；ch$\Delta=$ 素数 p 时，$\Delta\cong\mathbb{Z}_p$（含 p 个元）. 由此揭示出素域的构造. 且素域只能与素域同构. 特征为 ∞ 的素域都同构. 特征为素数 p 的素域都同构.

2）　任意域 E 有且只有一个素子域. 从而任意域都是素域的扩域.

事实上，由该命题已知域 E 必存在一个素子域. 设 Δ_1,Δ_2 都是 E 的素子域，则交 $\Delta_1\cap\Delta_2$ 既是 Δ_1 又是 Δ_2 的子域，但 Δ_1,Δ_2 都无真子域，于是 $\Delta_1=\Delta_1\cap\Delta_2=\Delta_2$. 所以 E 只有一个素子域.

---

①　张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 151. 定理 1.

②　北京大学数学系几何与代数教研室. 高等代数. 北京：高等教育出版社，1978

另一证法. 因域 E 的子域必存在(比如 E),故 E 的一切子域的交 Δ 必存在,这个交 Δ 就是 E 的一个素子域. 这是因为,Δ 是 E 的子域,又 Δ 本身是素域. 因为若 Δ 有子域 Δ',即 $\Delta'\subset\Delta$,则 Δ' 也是 E 的子域,但 Δ 是 E 的一切子域的交,从而 $\Delta'\supset\Delta$. 于是 $\Delta'=\Delta$,即 Δ 是素域. 所以 E 有素子域 Δ. 若 E 有两个素子域 Δ_1 与 Δ_2 且 $\Delta_1\neq\Delta_2$,即 Δ_1 不包含 Δ_2 或 Δ_2 不包含 Δ_1. 不妨设 Δ_1 不包含 Δ_2,则 $\exists\alpha\in\Delta_2$,但 $\alpha\overline{\in}\Delta_1$. 作 $\Delta=\Delta_1\cap\Delta_2$,$\Delta$ 是 Δ_2 的子域,又 $\alpha\in\Delta_2$,但 $\alpha\overline{\in}\Delta$,从而 Δ 是 Δ_2 的真子域,此与 Δ_2 是素域矛盾. 所以 E 只有一个素子域.

关于 E 的素子域的唯一性还可如下证明. 设 Δ_1,Δ_2 都是 E 的素子域且 $\Delta_1\neq\Delta_2$,则 $\Delta_1\cap\Delta_2$ 也是 Δ_1 的子域. 若 $\Delta_1\cap\Delta_2\neq\Delta_1$,则 $\Delta_1\cap\Delta_2$ 是 Δ_1 的真子域,此与 Δ_1 是素域矛盾;若 $\Delta_1\cap\Delta_2=\Delta_1$,则 $\Delta_1\subset\Delta_2$,此时 Δ_1 是 Δ_2 的真子域,与 Δ_2 是素域矛盾. 所以 E 的素子域唯一.

3) 利用域的特征可将域 E 分为两大类,$\mathrm{ch}\,E=\infty$ 与 $\mathrm{ch}\,E=$ 素数 p. 两类域的构造截然不同,而特征相同的域有许多相同的性质. 因此域的特征决定了域的代数结构.

4) 由该命题知特征为∞的域 E 含有一个与$\mathbb{Q}$同构的子域,从而 E 一定是无限域.

其逆否命题是:只含有限个元的有限域的特征必为一个素数. 也可如下证明:因有限域是一个有限加群,由第四章,二,7,特征定义知有限域的特征是一个素数①.

5) 设 E 是域 F 的扩域,Δ 是 F 的素子域,显然 Δ 也是 E 的素子域.

2. 设 $F(S)$ 是添加集 S 于域 F 所得的扩域,这里 F 是域 E 的子域,S 是 E 的子集. 证明:

$$F(S)=\left\{\frac{f_1(\alpha_1,\alpha_2,\cdots,\alpha_n)}{f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)}\middle|\begin{array}{c}\alpha_1,\alpha_2,\cdots,\alpha_n\in S,n\text{ 是正整数},f_1(\alpha_1,\alpha_2,\cdots,\alpha_n),\\ f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)(\neq 0)\in F[\alpha_1,\alpha_2,\cdots,\alpha_n]\end{array}\right\}.$$

证 记等号右面的集为 H. $\forall\dfrac{f_1(\alpha_1,\alpha_2,\cdots,\alpha_n)}{f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)}\in H$,因 $F(S)$ 是含 F 与 S 的域,故 $\dfrac{f_1(\alpha_1,\alpha_2,\cdots,\alpha_n)}{f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)}\in F(S)$,从而 $H\subset F(S)$. 反之,首先证明 H 是 E 的子域. 显然 $H\subset E$,$\exists$ 非零元 $1=\dfrac{1}{1}\in H$. $\forall\dfrac{f_1(\alpha_1,\alpha_2,\cdots,\alpha_n)}{f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)},\dfrac{g_1(\beta_1,\beta_2,\cdots,\beta_m)}{g_2(\beta_1,\beta_2,\cdots,\beta_m)}\in H$,因 $f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)g_2(\beta_1,\beta_2,\cdots,\beta_m)\neq 0$,故

$$\begin{aligned}&\frac{f_1(\alpha_1,\alpha_2,\cdots,\alpha_n)}{f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)}-\frac{g_1(\beta_1,\beta_2,\cdots,\beta_m)}{g_2(\beta_1,\beta_2,\cdots,\beta_m)}\\&=\frac{f_1(\alpha_1,\alpha_2,\cdots,\alpha_n)g_2(\beta_1,\beta_2,\cdots,\beta_m)-f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)g_1(\beta_1,\beta_2,\cdots,\beta_m)}{f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)g_2(\beta_1,\beta_2,\cdots,\beta_m)}\in H.\end{aligned}$$

同理,$\forall h_1,h_2\in H,h_2\neq 0,h_1h_2^{-1}\in H$. 于是 H 是 E 的子域. 又 $\forall a\in F,a=\dfrac{a}{1}\in H$,即 $F\subset H$. $\forall\theta\in S,\theta=\dfrac{\theta}{1}\in H$,即 $S\subset H$. 从而 H 是含 F 与 S 的域. 又 $F(S)$ 是含 F 与 S 的最小域,因此 $F(S)\subset H$. 所以 $F(S)=H$.

注 1) 构造一个域 F 的扩域的基本方法就是添加,添加就是把域 F 扩充为较大的域的一种手段.

2) $F(S)$ 是域 E 的含 F 与 S 的一切子域的交 K. 从而 E 的扩域 $F(S)$ 必存在.

---

① 张禾瑞. 近世代数基础. 北京:高等教育出版社,1978. 96. 定理 2.

事实上，由 $F(S)$是 E 的含 F 与 S 的子域，K 是 E 的含 F 与 S 的一切子域的交，有 $F(S)\supset K$. 反之，由 $F(S)$是 E 的含 F 与 S 的最小子域，K 是 E 的含 F 与 S 的子域，有 $F(S)\subset K$. 所以 $F(S)=K$.

3)　特别地，当 $S=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$是有限集时，由第十三章，三，4，7)，注②，扩域

$$F(\alpha_1,\alpha_2,\cdots,\alpha_n) = \left\{\frac{f_1(\alpha_1,\alpha_2,\cdots,\alpha_n)}{f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)}\,\middle|\, f_1(\alpha_1,\alpha_2,\cdots,\alpha_n),f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)(\neq 0)\in F[\alpha_1,\alpha_2,\cdots,\alpha_n]\right\}$$

是 F 上 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 的多项式环 $F[\alpha_1,\alpha_2,\cdots,\alpha_n]$的商域.

3. 命题：设 E 是域 F 的扩域，S_1,S_2 是 E 的子集，则

$$F(S_1)(S_2)=F(S_1\cup S_2)=F(S_2)(S_1).$$

主要说明什么问题？

答　主要说明一次添加与逐次添加所得的扩域相等，且与添加的顺序无关. 从而有

$$F(\alpha_1,\alpha_2,\cdots,\alpha_n)=F(\alpha_1)(\alpha_2)\cdots(\alpha_n).$$

因此可以利用单扩域来研究添加有限个元所得的扩域. 而添加一切集 S 中有限个元所得的扩域的并集就是扩域 $F(S)$(第十六章，二，1). 所以单扩域是扩域的基础.

4. 关于命题：设 E 是域 F 的扩域，$\alpha\in E$，则

(i)　单超越扩域 $F(\alpha)\cong F[x]$的商域 $F(x)$.

(ii)　单代数扩域 $F(\alpha)\cong F[x]/(p(x))$，其中 $p(x)$是 $F[x]$的最高系数为 1 的唯一确定的不可约多项式，且 $p(x)=0$[①].

1)　为何 $p(x)\neq 0$？

2)　为何 $p(x)$是 $F[x]$的最高系数为 1 的唯一确定的多项式？

3)　当 $F[x]$是域时，即当 α 是 F 上代数元时，为何 $F[\alpha]=F(\alpha)$？

4)　为何 $p(x)$是 $\ker\phi=(p(x))$中次数最低的多项式？

答　1)　因 α 是 F 上代数元，故 $\exists f(x)\in F[x]$，$f(x)\neq 0$，而 $f(\alpha)=0$. 于是 $\phi(f(x))=f(\alpha)=0$，即 $f(x)\in\ker\phi$，所以 $\ker\phi=(p(x))\neq\{0\}$. 因此 $p(x)\neq 0$.

2)　设 $p(x)=\varepsilon p_0(x)$，其中 ε 是 $p(x)$的最高系数，$p_0(x)$是最高系数为 1 的多项式. 因 $\varepsilon\neq 0$，故 ε 是域 F 的单位. 从而 $p(x)$与 $p_0(x)$相伴. 由第十四章，二，6，$(p(x))=(p_0(x))$. 因此我们可令 $p(x)$的最高系数是 1. 若 $\exists q(x)\in F[x]$，$q(x)$的最高系数也是 1，且 $(q(x))=(p(x))$. 则由第十四章，二，6，$q(x)=ap(x)$，其中 a 是 F 的单位. 因 $p(x)$，$q(x)$的最高系数都是 1，故 $a=1$. 从而 $q(x)=p(x)$. 所以 $p(x)$唯一.

3)　由第十六章，一，2，注 3)，$F(\alpha)=F[\alpha]$的商域. 今 $F[\alpha]$是域，由第十三章，二，5，$F[\alpha]$是 $F[\alpha]$自身的商域，所以 $F(\alpha)=F[\alpha]$.

另一证法. 因 $F[\alpha]$是含 F 和 α 的域，$F[\alpha]$是含 F 和 α 的最小域，故 $F(\alpha)\subset F[\alpha]$. 另一方面，显然 F 上 α 的多项式环 $F[\alpha]\subset$域 $F[(\alpha)$. 所以 $F[\alpha]=F(\alpha)$.

4)　$\forall s(x)(\neq 0)\in(p(x))$，有 $p(x)\,|\,s(x)$. 因 $s(x)\neq 0$，故 $\deg p(x)\leqslant\deg s(x)$.

注　1)　该命题给出了两类单扩域的结构. 利用添加的元是代数元还是超越元，可将域

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 155. 定理 1.

F 的扩域分成两大类.两类扩域的结构迥然不同.

2) 若 α 是域 F 上的代数元,则 $\exists F[x]$ 的最高系数为 1 的唯一确定的不可约多项式 $p(x)$ 且 $p(\alpha)=0$. 此 $p(x)$ 即为 α 在 F 上极小多项式.

3) 若 α 是 F 上代数元,则 $F(\alpha)=F[\alpha]$. 这是单代数扩域的特点. 当 α 是 F 上超越元时,$F(\alpha)\neq F[\alpha]$,但 $F(\alpha)\supset F[\alpha]$. 要注意圆括号与方括号的区别. 例,$\pi$ 是 $\mathbb{Q}$ 上超越元,

$$\mathbb{Q}(\pi)=\left\{\frac{\sum_{i=0}^{n}a_i\pi^i}{\sum_{j=0}^{m}b_j\pi^j}\,\middle|\,a_i,b_j\in\mathbb{Q}\ ,m,n\text{ 是非负整数},b_j\text{ 不全为 }0\right\},$$

$$\mathbb{Q}[\pi]=\left\{\sum_{i=0}^{n}a_i\pi^i\,\middle|\,a_i\in\mathbb{Q}\right\}.$$

显然 $\mathbb{Q}(\pi)\supsetneqq\mathbb{Q}[\pi]$.

4) 域 F 的单超越扩域必存在,且在同构意义下唯一.

事实上,由未定元存在定理[①],$\exists F$ 上未定元 x,从而 $\exists F$ 上 x 的多项式环 $F[x]$,于是 $\exists F[x]$ 的商域. 由第十六章,一,2,注 3),单扩域 $F(x)=F[x]$ 的商域. 又因 x 是 F 上超越元,故 $\exists F$ 的单超越扩域 $F(x)$. 由该定理,F 的任一单超越扩域 $F(\alpha)\cong F[x]$ 的商域 $F(x)$,所以 F 的单超越扩域在同构意义下唯一.

因此可知域 F 的单代数扩域必存在[②].

5) 该命题的证明可与前面题 1 中命题的证明相比较.

5. 关于命题:设 E 是域 F 的扩域,$\alpha\in E$,α 是 F 上代数元,$F(\alpha)\cong F[x]/(p(x))$,其中 $p(x)$ 是 α 在 F 上极小多项式,则

(i) $\forall\beta\in F(\alpha)$,$\beta$ 可唯一表成 $\beta=\sum_{i=0}^{n-1}a_i\alpha^i$,其中 $a_i\in F$,$n=\deg p(x)$.

(ii) $f(\alpha)=\sum_{i=0}^{n-1}a_i\alpha^i$, $g(\alpha)=\sum_{i=0}^{n-1}b_i\alpha^i\in F(\alpha)$, $f(\alpha)+g(\alpha)=\sum_{i=0}^{n-1}(a_i+b_i)\alpha^i$.

(iii) $\forall f(\alpha),g(\alpha)\in F(\alpha)$, $f(\alpha)g(\alpha)=r(\alpha)$,其中 $r(\alpha)\in F(\alpha)$ 且 $r(x)$ 是 $f(x)g(x)$ 除以 $p(x)$ 所得的余式.[③]

1) 为何 β 的表法唯一?

2) 证明(iii).

答 1) 若 $\beta=r_1(\alpha)=r_2(\alpha)$,$r_1(x)=0$ 或 $\deg r_1(x)<n$,$r_2(x)=0$ 或 $\deg r_2(x)<n$. 令 $k(x)=r_1(x)-r_2(x)$,则 $k(x)=0$ 或 $\deg k(x)<n$. 于是 $\phi(k(x))=k(\alpha)=r_1(\alpha)-r_2(\alpha)=0$[④],因此 $k(x)\in\ker\phi=(p(x))$,从而 $p(x)\mid k(x)$. 所以 $k(x)=0$. 否则,与 $\deg k(x)<n=\deg p(x)$ 矛盾. 即 $r_1(x)=r_2(x)$. 可见 β 的表法唯一.

2) 事实上,由第十五章,一,2 中命题,$f(x)g(x)=q(x)p(x)+r(x)$,其中 $q(x),r(x)\in F[x]$,$r(x)=0$ 或 $\deg r(x)<\deg p(x)$. 所以 $f(\alpha)g(\alpha)=q(\alpha)p(\alpha)+r(\alpha)=r(\alpha)$[⑤].

---

① 张禾瑞. 近世代数基础. 北京:高等教育出版社,1978. 103. 定理 1.

② 同上. 158. 定理 3.

③ 同上. 156. 定理 2

④⑤ 同上. 108. 定理 3.

注　单代数扩域 $F(\alpha)\cong F[x]/(p(x))$，由此看来，$F(\alpha)$中的元似乎比较抽象，复杂. 实际上，$F(\alpha)$中的元很具体，简单. $F(\alpha)=\left\{\sum_{i=0}^{n-1}a_i\alpha^i\,\middle|\,a_i\in F\right\}$，其中 $n=\deg p(x)$. 这就更进一步地表明了对于单代数扩域 $F(\alpha)$来说，α在F上极小多项式$p(x)$的重要作用，它唯一确定了$F(x)$的构造.

6. 1)　元α在域F上极小多项式的定义是什么?

2)　给出一些元α在域F上极小多项式的等价形式.

答　1)　设E是域F的扩域，$\alpha\in E$，则

$p(x)$是α在F上极小多项式 $\Leftrightarrow$

(i)　$p(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0\in F[x]$；

(ii)　$p(\alpha)=0$；

(iii)　$\forall\, s(x)(\neq 0)\in F[x], s[\alpha]=0$，有 $\deg p(x)\leqslant\deg s(x)$

且称 $n=\deg p(x)$为α在F上的次数.

2)　设E是域F的扩域，$\alpha\in E$，则

$p(x)$是α在F上极小多项式

$\overset{(1)}{\Leftrightarrow}$(i)　$p(x)$是F上最高系数为1的多项式；

(ii)　$p(\alpha)=0$；

(iii)　$\forall\, s(x)\in F[x]$，$s(\alpha)=0$，有 $p(x)\mid s(x)$.

$\overset{(2)}{\Leftrightarrow}$(i)　同上；

(ii)　同上；

(iii)　$p(x)$在F上不可约.

$\overset{(3)}{\Leftrightarrow}$(i)　同上；

(ii)　同上；

(iii)　$(F(\alpha):F)=\deg p(x)=n$.

事实上，(1)　($\Rightarrow$)　(i)与(ii)显然成立. 由第十五章，一，2中命题，$s(x)=p(x)q(x)+r(x)$，其中 $q(x),r(x)\in F[x]$，$r(x)=0$ 或 $\deg r(x)<\deg p(x)$. 于是 $s(\alpha)=p(\alpha)q(\alpha)+r(\alpha)$①. 因 $s(\alpha)=p(\alpha)=0$，故 $r(\alpha)=0$. 若 $r(x)\neq 0$，则 $\deg r(x)<\deg p(x)$，此与$p(x)$是α在F上极小多项式矛盾，从而 $r(x)=0$，即 $s(x)=p(x)q(x)$. 所以 $p(x)\mid s(x)$. 于是(iii)成立.

($\Leftarrow$)　由(iii)，$\forall\, s(x)(\neq 0)\in F[x], s(\alpha)=0$，有 $\deg p(x)\leqslant\deg s(x)$. 从而由定义知，$p(x)$是$\alpha$在$F$上极小多项式.

(2)　($\Rightarrow$)　(i)，(ii)显然成立. 若$p(x)$在F上不是不可约. 因$p(x)$是α在F上极小多项式，故 $p(x)\neq 0$ 且 $p(x)\neq F[x]$的单位，不然，若 $p(x)=F[x]$的单位，则 $p(x)\in F$，从而 $p(x)=1$，因此 $p(\alpha)=1\neq 0$，矛盾. 所以 $p(x)\neq F[x]$的单位. 于是在域F上$p(x)$可约. 由第十五章，一，4，注3)，$p(x)=g(x)h(x)$，其中 $g(x),h(x)\in F[x]$，$0<\deg g(x)<\deg p(x)$，

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 108. 定理3.

$0<\deg h(x)<\deg p(x)$. 所以 $0=p(\alpha)=g(\alpha)h(\alpha)$. 因 $g(\alpha),h(\alpha)\in F[\alpha]$，又 $F[\alpha]$是整环，无零因子，故 $g(\alpha)=0$ 或 $h(\alpha)=0$. 但 $\deg g(x)<\deg p(x)$且 $\deg h(x)<\deg p(x)$，此与 $p(x)$是 α 在 F 上极小多项式矛盾. 所以 $p(x)$在 F 上不可约.

($\Leftarrow$) 由(i)，(ii)知 α 是 F 上代数元，从而 α 在 F 上极小多项式必存在. 设 $t(x)$是 α 在 F 上极小多项式，则由 $p(\alpha)=0$，利用等价形式(1)，$t(x)\mid p(x)$，因 $p(x)$在 F 上不可约，又 $t(x)\neq F[x]$的单位，故 $t(x)$是 $p(x)$的相伴元，即 $t(x)=\varepsilon p(x)$，ε 是 F 的单位. 因 $t(x)$，$p(x)$的最高系数都是 1，故 $\varepsilon=1$，即 $p(x)=t(x)$. 所以 $p(x)$是 α 在 F 上极小多项式.

(3) ($\Rightarrow$) (i)，(ii)显然成立. 因 $p(x)$是 α 在 F 上 n 次极小多项式，故 $F(\alpha)$是 F 的单代数扩域. 从而$(F(\alpha):F)=\deg p(x)=n$[①]. 所以(iii)成立.

($\Leftarrow$) 因$(F(\alpha):F)=n$，故 α 在 F 上极小多项式的次数为 n[②]. 今已知 $\deg p(x)=n$，$p(x)$的最高系数是 1，$p(\alpha)=0$，即 $p(x)$是 F 上以 α 为根的非零多项式中次数最低者，所以由定义，$p(x)$是 α 在 F 上极小多项式.

注 1) 设 $p(x)$是 α 在域 F 上极小多项式，而 $\alpha\in F$，则 $p(x)=x-\alpha$.

2) 若 α 是域 F 上超越元，则 α 在 F 上极小多项式不存在. 否则，若有 $p(x)$是 α 在 F 上极小多项式，则 $p(x)\neq 0$，$p(x)\in F[x]$，$p(\alpha)=0$，此与 α 是 F 上超越元矛盾.

该命题的逆否命题是：若存在 α 在域 F 上极小多项式，则 α 是 F 上代数元.

3) 若 α 是域 F 上代数元，则 α 在 F 上极小多项式必存在.

4) 同一元的极小多项式与域有关. 例如，$\sqrt{2}$在$\mathbf{Q}$上极小多项式是 x^2-2，而在$\mathbf{R}$上极小多项式是 $x-\sqrt{2}$.

5) α 在域 F 上极小多项式唯一.

事实上，若 $p(x)$与 $q(x)$都是 α 在 F 上极小多项式，当然次数都是 n，最高系数都是 1，$p(\alpha)=q(\alpha)=0$. 若 $q(x)\neq p(x)$，则 $h(x)=g(x)-p(x)\neq 0$，且 $\deg h(x)<n$. 但 $h(\alpha)=q(\alpha)-p(\alpha)=0$. 此与 $p(x)$是 F 上极小多项式矛盾. 所以 α 在域 F 上极小多项式唯一.

另一证法，若 $p(x)$与 $q(x)$都是 α 在 F 上极小多项式. 由等价形式(1)，$p(x)\mid q(x)$，$q(x)\mid p(x)$. 从而 $p(x)$与 $q(x)$相伴，即 $p(x)=\varepsilon q(x)$，其中 ε 是 F 的单位. 因 $p(x)$，$q(x)$的最高系数都是 1，故 $\varepsilon=1$，即 $p(x)=q(x)$.

6) 设 α 是域 F 上代数元，则

α 在 F 上的次数$=\alpha$ 在 F 上极小多项式的次数$=$扩域 $F(\alpha)$在 F 上的次数$(F(\alpha):F)=$ $F(\alpha)$在 F 上的维数，这三个次数统一起来了.

7) 设 E 是域 F 的扩域，α 是 F 上代数元，$p(x)$是 α 在 F 上极小多项式，$q(x)$是 α 在 E 上极小多项式，则在 $E[x]$中，$q(x)\mid p(x)$.

与等价形式(1)必要性的证明类似地可证该命题. 但用同样的证法却不能证明 $p(x)\mid q(x)$，请读者考虑其中原因.

7. 证明：设 $F(\alpha)$，$F(\beta)$都是域 F 的单代数扩域，α,β 在 F 上有相同的极小多项式$p(x)$，

①② 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 163. 推论 2.

则 $F(\alpha)\cong F(\beta)$[①].

证一　设 $\deg p(x)=n$,显然 $n>0$. ,由第十六章,一,5 中命题,

$$F(\alpha)=\left\{\sum_0^{n-1}a_i\alpha^i \,\middle|\, a_i\in F\right\},\quad F(\beta)=\left\{\sum_0^{n-1}b_i\beta^i \,\middle|\, b_i\in F\right\}.$$

设ϕ: $\sum_0^{n-1}a_i\alpha^i \to \sum_0^{n-1}a_i\beta^i$,则$\phi$是 $F(\alpha)$ 与 $F(\beta)$ 间的一个同构映射. 事实上,$\forall f(\alpha)=\sum_0^{n-1}a_i\alpha^i\in F(\alpha)$,由第十六章,一,5 中命题,$f(\alpha)$的表法唯一,知 $\exists|\, f(\beta)=\sum_0^{n-1}a_i\beta^i\in F(\beta)$,使得 $\phi(f(\alpha))=f(\beta)$,即ϕ是映射. ϕ显然是满射. $\forall g(\beta)=\sum_0^{n-1}b_i\beta^i\in F(\beta)$,同理,$g(\beta)$的表法唯一,知 $g(\beta)$在ϕ下的逆象 $\sum_0^{n-1}b_i\alpha^i$ 唯一. 所以ϕ是一一映射. $\forall f(\alpha),g(\alpha)\in F(\alpha)$,由第十五章,一,2 中命题,$f(x)g(x)=p(x)q(x)+r(x)$,其中 $q(x),r(x)\in F[x]$,$r(x)=0$ 或$\deg r(x)<\deg p(x)=n$,从而 $r(x)=\sum_0^{n-1}c_ix^i$,$c_i\in F$. 因 α,β在 F 上有相同的极小多项式$p(x)$,即 $p(\alpha)=p(\beta)=0$,故

$$\phi:\ f(\alpha)g(\alpha)=r(\alpha)=\sum_0^{n-1}c_i\alpha^i \to \sum_0^{n-1}c_i\beta^i=r(\beta)=f(\beta)g(\beta).$$

所以 $F(\alpha)\overset{\phi}{\cong} F(\beta)$.

证二　由第十六章,一,4 中命题,

$$F(\alpha)\cong F[x]/(p(x)),\quad F(\beta)\cong F[x]/(p(x)).$$

所以 $F(\alpha)\cong F(\beta)$.

注　1)　举个例子,$\mathbf{Q}(\sqrt[3]{5})$,$\mathbf{Q}(\omega\sqrt[3]{5})$都是有理数域$\mathbf{Q}$的单代数扩域,$\sqrt[3]{5}$,$\omega\sqrt[3]{5}$在$\mathbf{Q}$上有相同的极小多项式 x^3-5,由该命题,$\mathbf{Q}(\sqrt[3]{5})\cong\mathbf{Q}(\omega\sqrt[3]{5})$,其中 $\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}$.

因此,一个不可约多项式的任意两个根具有许多相同的性质. 根的代数性质可以从它所满足的不可约多项式推导出来.

2)　若将该命题中的条件"α,β在 F 上有相同的极小多项式 $p(x)$"改成"α,β在 F 上的次数相等",命题不成立. 即:设 $F(\alpha)$,$F(\beta)$都是域 F 的单代数扩域,$(F(\alpha):F)=(F(\beta):F)$,未必有 $F(\alpha)\cong F(\beta)$.

例　$\mathbf{Q}(\mathrm{i})$,$\mathbf{Q}(\sqrt{2})$都是$\mathbf{Q}$的单代数扩域,i,$\sqrt{2}$在$\mathbf{Q}$上极小多项式分别是 x^2+1,x^2-2,因此$(\mathbf{Q}(\mathrm{i}):\mathbf{Q})=(\mathbf{Q}(\sqrt{2}):\mathbf{Q})=2$. 但$\mathbf{Q}(\mathrm{i})$与$\mathbf{Q}(\sqrt{2})$不同构. 不然,假设$\mathbf{Q}(\mathrm{i})\overset{\phi}{\cong}\mathbf{Q}(\sqrt{2})$,则 ϕ:$1\to1$,$-1\to-1$. 设ϕ:$\mathrm{i}\to a+b\sqrt{2}$,则 $\mathrm{i}^2=-1\to(a+b\sqrt{2})^2=-1$. 从而 $a+b\sqrt{2}=\pm\mathrm{i}$,此为不可能. 所以$\mathbf{Q}(\mathrm{i})$与$\mathbf{Q}(\sqrt{2})$不同构.

因此在该命题的证明中,要注意 α,β在 F 上有相同的极小多项式 $p(x)$这一条件的作用.

又例　$\mathbf{Q}(\mathrm{i})$,$\mathbf{Q}(\omega)$都是$\mathbf{Q}$的单代数扩域,i,$\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}$ 在$\mathbf{Q}$上极小多项式分别是

① 张禾瑞. 近世代数基础. 北京:高等教育出版社,1978. 159. 定理 4.

x^2+1, x^2+x+1，从而$(\mathbf{Q}(\mathrm{i}):\mathbf{Q})=(\mathbf{Q}(\omega):\mathbf{Q})=2$. 但$\mathbf{Q}(\mathrm{i})$与$\mathbf{Q}(\omega)$不同构. 否则，假设$\mathbf{Q}(\mathrm{i})\overset{\phi}{\cong}\mathbf{Q}(\omega)$，则$\phi: -1\to -1$. 设$\phi: \mathrm{i}\to a+b\omega$，则$\mathrm{i}^2=-1\to(a+b\omega)^2=-1$，即$a+b\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}\right)=\pm\mathrm{i}$. 于是$a-\frac{b}{2}+\left(\frac{b\sqrt{3}}{2}\pm1\right)\mathrm{i}=0$. $\frac{b\sqrt{3}}{2}=\pm1$，$b=\frac{\pm2}{\sqrt{3}}$，因b是有理数，故发生矛盾. 所以$\mathbf{Q}(\mathrm{i})$与$\mathbf{Q}(\omega)$不同构.

又例 $\mathbf{Q}(\sqrt{2})$，$\mathbf{Q}(\sqrt{3})$都是$\mathbf{Q}$的单代数扩域，$\sqrt{2}$，$\sqrt{3}$在$\mathbf{Q}$上极小多项式分别是x^2-2，x^2-3，从而$(\mathbf{Q}(\sqrt{2}):\mathbf{Q})=(\mathbf{Q}(\sqrt{3}):\mathbf{Q})=2$. 但$\mathbf{Q}(\sqrt{2})$与$\mathbf{Q}(\sqrt{3})$不同构（参看第十一章，四，11）.

3) 设$F(\alpha)$，$F(\beta)$都是域F的单代数扩域. 将$F(\alpha)$，$F(\beta)$看成域F上的向量空间，若$(F(\alpha):F)=(F(\beta):F)$，即$F(\alpha)$，$F(\beta)$在域$F$上的维数相等，同《高等代数》[①]中结论一样，有域F上向量空间$F(\alpha)$与向量空间$F(\beta)$同构. 但域$F(\alpha)$与域$F(\beta)$未必同构，此由注2)中三个例子可见.

4) 该命题的逆命题不成立，即：设$F(\alpha)$，$F(\beta)$都是域F的单代数扩域，且$F(\alpha)\cong F(\beta)$，但α，β在F上的极小多项式未必相同. 见第十六章，二，3. 下面再举些例子.

例 $\mathbf{Q}(\sqrt{3}\,\mathrm{i})$，$\mathbf{Q}(\omega)$都是$\mathbf{Q}$的单代数扩域，$\sqrt{3}\,\mathrm{i}$，$\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}$在$\mathbf{Q}$上极小多项式分别是$x^2+3$，$x^2+x+1$. 而$\mathbf{Q}(\sqrt{3}\,\mathrm{i})=\mathbf{Q}(\omega)$. 事实上，

$$\sqrt{3}\,\mathrm{i}=2\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}\right)+1=2\omega+1\in\mathbf{Q}(\omega).$$

因$\mathbf{Q}(\sqrt{3}\,\mathrm{i})$是含$\mathbf{Q}$，$\sqrt{3}\,\mathrm{i}$的最小域，$\mathbf{Q}(\omega)$是含$\mathbf{Q}$，$\sqrt{3}\,\mathrm{i}$的域，故$\mathbf{Q}(\sqrt{3}\,\mathrm{i})\subset\mathbf{Q}(\omega)$. 反之，$\omega=-\frac{1}{2}+\frac{1}{2}(\sqrt{3}\,\mathrm{i})\in\mathbf{Q}(\sqrt{3}\,\mathrm{i})$，同上理，有$\mathbf{Q}(\omega)\subset\mathbf{Q}(\sqrt{3}\,\mathrm{i})$. 所以$\mathbf{Q}(\sqrt{3}\,\mathrm{i})=\mathbf{Q}(\omega)$，显然$\mathbf{Q}(\sqrt{3}\,\mathrm{i})\cong\mathbf{Q}(\omega)$.

由第十六章，一，4中命题，$\mathbf{Q}[x]/(x^2+3)\cong\mathbf{Q}[x]/(x^2+x+1)$.

又例 $\mathbf{Q}(\sqrt{2})=\mathbf{Q}(2\sqrt{2})$，$\sqrt{2}$，$2\sqrt{2}$在$\mathbf{Q}$上极小多项式分别是$x^2-2$，$x^2-8$. $\mathbf{Q}[x]/(x^2-2)\cong\mathbf{Q}[x]/(x^2-8)$.

又例 $\mathbf{Q}(-2+\sqrt{2})=\mathbf{Q}(\sqrt{2})$，$-2+\sqrt{2}$，$\sqrt{2}$在$\mathbf{Q}$上极小多项式分别是$x^2+4x+2$，$x^2-2$. $\mathbf{Q}[x]/(x^2+4x+2)\cong\mathbf{Q}[x]/(x^2-2)$.

8. 试给出域F上向量空间，线性相(无)关，n维向量空间(有限维空间)，基，无限维空间的定义.

答 设E是加群，F是域，且∃一个$F\times E$到E的映射ϕ叫做乘法. $\forall a\in F, \alpha\in E$，把$\phi(a,\alpha)$记为$a\alpha$，$\forall a,b\in F$，$\alpha,\beta\in E$，有

1) $1\alpha=\alpha$，其中1是F的单位元；

2) $(ab)\alpha=a(b\alpha)$；

3) $(a+b)\alpha=a\alpha+b\alpha$；

① 北京大学数学系几何与代数教研室. 高等代数. 北京：高等教育出版社，1978

4)　$a(\alpha+\beta)=a\alpha+a\beta$.

则称 E 是 F 上的一个向量空间.

若 E 是域 F 的扩域,显然 E 是 F 上的一个向量空间.

设 E 是域 F 上的向量空间.对于 $\alpha_1,\alpha_2,\cdots,\alpha_r\in E$,若 $\exists(\bar{\exists})$ 不全为零的元 $a_1,a_2,\cdots,a_r\in F$,使得

$$a_1\alpha_1+a_2\alpha_2+\cdots+a_r\alpha_r=0.$$

则说 $\alpha_1,\alpha_2,\cdots,\alpha_r$ 对于 F 来说线性(无)关.

设 E 是域 F 上的向量空间.若

1)　$\exists\alpha_1,\alpha_2,\cdots,\alpha_n(\in E)$ 对于 F 来说线性无关,这里 n 是正整数;

2)　$\forall\beta\in E,\beta,\alpha_1,\alpha_2,\cdots,\alpha_n$ 对于 F 来说线性相关.

则说 E 是 F 上的 n 维向量空间,也说 E 是 F 上的有限维空间.说 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 E 在 F 上的一个基.若 E 含有任意多个对于 F 来说线性无关的元,则说 E 是 F 上的无限维空间.

注　1)　为了这里的需要,我们给出下面命题:

设 E 是域 F 上的向量空间,$\alpha_1,\alpha_2,\cdots,\alpha_n\in E$,则

$\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 E 在 F 上的一个基

$\Leftrightarrow$ ①　$\alpha_1,\alpha_2,\cdots,\alpha_n$ 对于 F 来说线性无关;

②　$\forall\beta\in E$,有 $\beta=\sum_{i=1}^{n}a_i\alpha_i$,其中 $a_i\in F$.

$\Leftrightarrow\forall\beta\in E$,$\beta$ 都可唯一地表为 $\beta=\sum_{i=1}^{n}a_i\alpha_i,a_i\in F$.

设 E 是域 F 上的 n 维向量空间,则 E 中任意 $n+1$ 个元对于 F 来说都线性相关.

仿《高等代数》[①]中的证明可证.

2)　在《高等代数》[②]中,数域上一个向量空间如果含有一个非零向量,那么它一定含有无限多个向量.把域 F 的扩域 E 看作 F 上的向量空间时,此结论不成立.

例　$\mathbb{Z}_p$(p 是素数)是域 $\mathbb{Z}_p$上的向量空间,$\mathbb{Z}_p$显然含单位元$[1]\neq[0]$,但 $\mathbb{Z}_p$恰含 p 个元.

请读者考虑产生此区别的关键原因为何?

9. 关于定理:设 E 是域 I 的有限扩域,I 是域 F 的有限扩域,则 E 也是 F 的有限扩域,且$(E:F)=(E:I)(I:F)$[③].

1)　该定理的作用为何?

2)　证明该定理的逆命题:设 E 是域 I 的扩域,I 是域 F 的扩域,且 E 是 F 的有限扩域,则 I 是 F 的有限扩域,E 是 I 的有限扩域.

答　1)　该定理是域论中的一个重要的十分有用的定理,称定理中的等式为域的基本次数公式.它起着与群论中的 Lagrange 定理类似的作用.说明有限扩域可以传递.

2)　事实上,假设 I 是 F 的无限扩域,又 $E\supset I$,则在 I 中从而在 E 中有任意多个对于 F 来说的线性无关的元.于是 E 是 F 的无限扩域,此与已知矛盾.所以 I 是 F 的有限

---

①② 北京大学数学系几何与代数教研室.高等代数.北京:高等教育出版社,1978

③　张禾瑞.近世代数基础.北京:高等教育出版社,1978.161.定理 1.

扩域.

若$(E:F)=s$.假设E是I的无限扩域,则$\exists s+1$个元$\alpha_1,\alpha_2,\cdots,\alpha_{s+1}(\in E)$对于$I$来说线性无关.下面证明$\alpha_1,\alpha_2,\cdots,\alpha_{s+1}$对于$F$来说也线性无关.设$b_1\alpha_1+b_2\alpha_2+\cdots+b_{s+1}\alpha_{s+1}=0$,$b_i\in F$.因$F\subset I$,故$b_i\in I$,从而$b_i=0,i=1,2,\cdots,s+1$.因此$E$中$s+1$个元$\alpha_1,\alpha_2,\cdots,\alpha_{s+1}$对于$F$来说线性无关.此与$(E:F)=s$矛盾.所以$E$是$I$的有限扩域.[另一证法,因$E$是$F$的有限扩域,$I$是$F$的有限扩域,故由第十六章,二,9,$\exists\alpha_1,\alpha_2,\cdots,\alpha_n\in E$,$\exists\beta_1,\beta_2,\cdots\beta_m\in I$,使得$F(\alpha_1,\alpha_2,\cdots,\alpha_n)=E$,$F(\beta_1,\beta_2,\cdots,\beta_m)=I$,于是

$$\begin{aligned}I(\alpha_1,\alpha_2,\cdots,\alpha_n)&=F(\beta_1,\beta_2,\cdots,\beta_m)(\alpha_1,\alpha_2,\cdots,\alpha_n)\\&=F(\alpha_1,\alpha_2,\cdots,\alpha_n)(\beta_1,\beta_2,\cdots,\beta_m)\\&=E(\beta_1,\beta_2,\cdots,\beta_m)\\&=E(\text{因 }\beta_j\in E).\end{aligned}$$

因α_i是F上代数元且$I\supset F$,故α_i也是I上代数元,$i=1,2\cdots,n$.所以E是I的有限扩域.[1]]

注 1) 设E是域F的有限扩域,$\forall\alpha\in E$,则$(F(\alpha):F)\mid(E:F)$,即α在F上的次数整除E在F上的次数.

事实上,由第十六章,一,10,α是F上代数元,从而$F(\alpha)$是F的有限扩域.由本题2),E是$F(\alpha)$的有限扩域,于是$(E:F)=(E:F(\alpha))(F(\alpha):F)$.又$(E:F(\alpha))$是正整数,从而$(F(\alpha):F)\mid(E:F)$.

2) 设E是域I的扩域,I是域F的扩域,且E是F的有限扩域,则$(E:I)\mid(E:F)$,$(I:F)\mid(E:F)$.

事实上,由本命题2)及该命题,有$(E:F)=(E:I)(I:F)$,从而结论成立.

3) 用数学归纳法可以证明:设F_{i+1}是域F_i的扩域,$i=1,2,\cdots,n$,且F_{n+1}是F_1的有限扩域,则F_{i+1}是F_i的有限扩域.

4) 设E是域I的扩域,I是域F的扩域,且E是F的有限扩域,$\alpha\in E$,则$I(\alpha)$是$F(\alpha)$的有限扩域.

事实上,因E是F的有限扩域,又$E\supset I(\alpha)\supset F$,故由本命题2),$I(\alpha)$是$F$的有限扩域,又$I(\alpha)\supset F(\alpha)\supset F$,再由本命题2),$I(\alpha)$是$F(\alpha)$的有限扩域.

10. 给出命题:设I是域F的有限扩域,则I是F的代数扩域[2].其逆否命题是什么?

答 设I不是F的代数扩域,则I不是F的有限扩域.即:设S是域E的子集,F是E的子域,α是F上超越元,$\alpha\in S$,则$F(S)$不是F的代数扩域,从而$F(S)$是F的无限扩域.

例 $\mathbb{R}$是$\mathbb{Q}$的无限扩域,因有$\mathbb{Q}$上超越元$\pi\in\mathbb{R}$.

当然,特别地,若α是域F上超越元,则添加有限个元$\alpha,\alpha_1,\alpha_2,\cdots,\alpha_n$于域$F$所得的扩域$F(\alpha,\alpha_1,\alpha_2,\cdots,\alpha_n)$是$F$的无限扩域.

更特别地,设域$E=F(\alpha)$是域F的单扩域,则

$$E\text{ 是 }F\text{ 的无限扩域}\Leftrightarrow\alpha\text{ 是 }F\text{ 上超越元}.$$

事实上,$(\Rightarrow)$ 略.

---

① 张禾瑞.近世代数基础.北京:高等教育出版社,1978.163.定理3.

② 同上,163.推论3.

(⇐)　由该命题可知.

11. 1)　证明:设 α,β 是域 F 上代数元,则 $\alpha \pm \beta, \frac{\alpha}{\beta}(\beta\neq 0)$ 也是 F 上代数元[①].

2)　证明:在域 F 的任意扩域 E 中,F 上的在 E 中的全体代数元作成的集 K 是 E 的一个子域. 且 K 是 F 的代数扩域.

3)　举例说明上面 10 题中命题的逆命题不成立. 即,域 F 的代数扩域未必是 F 的有限扩域. 因此代数扩域是比有限扩域更广泛的一类扩域.

证　1)　因 α,β 是 F 上代数元,故 $F(\alpha,\beta)$ 是 F 的代数扩域. 因 $\alpha \pm \beta, \frac{\alpha}{\beta}(\beta\neq 0)\in F(\alpha,\beta)$,故 $\alpha \pm \beta, \frac{\alpha}{\beta}(\beta\neq 0)$ 是 F 上代数元.

2)　因域 F 中的元 a 都是 E 中的在 F 上代数元,即 $a\in K$,故 $E\supset K\neq\phi$,且 K 中含 $\neq 0$ 的元. $\forall \alpha,\beta\in K$, $\alpha-\beta\in K$, $\beta\neq 0$ 时,$\alpha\beta^{-1}=\frac{\alpha}{\beta}\in K$,所以 K 是 E 的子域. 显然 K 是 F 的代数扩域.

3)　**例 1**　由该题 2)知,在 $\mathbb{Q}$ 上为代数元的一切复数作成的集 K 是 $\mathbb{Q}$ 的代数扩域. 但 K 不是 $\mathbb{Q}$ 的有限扩域.

事实上,对于 $\mathbb{Q}$ 上任意一个最高系数为 1 的不可约多项式 $p(x)$,设 $\deg p(x)=n$. 则 $\exists\, \mathbb{Q}$ 的单代数扩域 $\mathbb{Q}(\alpha)$,且 $p(x)$ 是 α 在 $\mathbb{Q}$ 上极小多项式. 从而 $1,\alpha,\cdots,\alpha^{n-1}$ 是向量空间 $\mathbb{Q}(\alpha)$ 在 $\mathbb{Q}$ 上的一个基,即 $1,\alpha,\cdots,\alpha^{n-1}(\in\mathbb{Q}(\alpha)\subset K)$ 对于 $\mathbb{Q}$ 来说线性无关. 由于 $\mathbb{Q}$ 上有任意高次的不可约多项式(如 $x^n+2\in\mathbb{Q}[x]$),于是 K 有任意有限多个对于 $\mathbb{Q}$ 来说线性无关的元,所以 K 是 $\mathbb{Q}$ 的无限扩域.

另一证法,若 K 是 $\mathbb{Q}$ 的有限扩域,设 $(K:\mathbb{Q})=n$. 由艾森斯坦因不可约性判别准则(第十五章,四,13)知,$n+1$ 次多项式 $p(x)=x^{n+1}+2x+2$ 在 $\mathbb{Q}$ 上不可约. 设 $\alpha(\in K)$ 是 $p(x)$ 的一个根,则 $p(x)$ 是 α 在 $\mathbb{Q}$ 上极小多项式,从而 $n+1$ 个元 $1,\alpha,\cdots,\alpha^n(\in K)$ 对于 $\mathbb{Q}$ 来说线性无关. 此与 $(K:\mathbb{Q})=n$ 矛盾. 所以 K 不是 $\mathbb{Q}$ 的有限扩域.

例 2　因 $\sqrt{2},\sqrt[3]{2},\sqrt[4]{2},\cdots,\sqrt[n]{2},\cdots$ 都是 $\mathbb{Q}$ 上代数元,故 $E=\mathbb{Q}(\sqrt{2},\sqrt[3]{2},\sqrt[4]{2},\cdots,\sqrt[n]{2},\cdots)$ 是 $\mathbb{Q}$ 的代数扩域. 而在无限多个元 $\sqrt{2},\sqrt[3]{2},\sqrt[4]{2},\cdots,\sqrt[n]{2},\cdots$ 中任意有限个元对于 $\mathbb{Q}$ 来说都线性无关,因此 E 是 $\mathbb{Q}$ 的无限扩域.

例 3　设 p 是任意素数,因 $\sqrt{p}$ 是 $\mathbb{Q}$ 上不可约多项式 x^2-p 的根,故 $\sqrt{p}$ 是 $\mathbb{Q}$ 上代数元. 从而 $E=\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5},\cdots,\sqrt{p},\cdots)$ 是 $\mathbb{Q}$ 的代数扩域. 与例 2 同理,E 不是 $\mathbb{Q}$ 的有限扩域.

12. 设 E 是域 F 的扩域,证明:

$$(E:F)=1 \Leftrightarrow E=F.$$

从而 E 是 E 的 1 次扩域.

证　(⇒)　因 $(E:F)=1$,故 $\exists\,\alpha\in E$, $\alpha\neq 0$, α 是 E 在 F 上的基. 取 $a(\neq 0)\in F\subset E$,必有 $b(\neq 0)\in F$,使 $a=b\alpha$. 因 F 是域,故 $\alpha=b^{-1}a\in F$. 从而 E 在 F 上的基 α 必然 $\in F$. 因此 $\forall \beta\in E$,有 $\beta=c\alpha$, $c\in F$,即 $\beta\in F$,从而 $E\subset F$,显然 $F\subset E$. 所以 $E=F$.

---

① 张禾瑞. 近世代数基础. 北京:高等教育出版社,1978. 163. 推论 4.

(⇐) E 的单位元 $1(\neq 0)$ 对于 F 来说线性无关. $\forall \beta \in E$,有 $\beta=\beta 1$. 因 $E=F$,故等式右边的 $\beta \in F$. 从而 1 是 E 在 F 上的基,于是 $(E:F)=1$.

注 当 E 是域 F 的扩域时,利用该命题可证明 $E=F$.

二、典型问题分析

1. 证明:$F(S)$ 的一切添加 S 的有限子集于 F 所得的子域的并集是一个域.

证一 设 $M=\left\{F(A) \middle| A \text{ 是 } S \text{ 的有限子集}\right\}$,$K=\bigcup\limits_{F(A)\in M} F(A)$. 而 $K=F(S)$. 事实上,因 $F(A)$ 是含 F 与 A 的最小域,$F(S)$ 是含 F 与 A 的域,故 $F(A)\subset F(S)$,从而 $K\subset F(S)$. 反之,$\forall \alpha \in F(S)$,有 $\alpha=\dfrac{f_1(\alpha_1,\alpha_2,\cdots,\alpha_n)}{f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)}\in F(\alpha_1,\alpha_2,\cdots,\alpha_n)$. 因 M 中的 A 是 S 的一切有限子集,故 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)\subset K$,于是 $\alpha\in K$,即 $F(S)\subset K$. 所以 $K=F(S)$. 因此 K 是一个域.

证二 设 $M=\left\{F(A) \middle| A \text{ 是 } S \text{ 的有限子集}\right\}$,$K=\bigcup\limits_{F(A)\in M} F(A)$. 下面证明 K 是 $F(S)$ 的子域. 由证一知 $K\subset F(S)$. K 有非零元 1. $\forall \alpha,\beta\in K$,必 $\exists F(A),F(B)$,使得 $\alpha\in F(A)$,$\beta\in F(B)$. 因 $A\cup B$ 也是 S 的有限子集,故 $\alpha-\beta\in F(A\cup B)\subset K$. 若 $\beta\neq 0$,$\beta\in F(B)$,因 $F(B)$ 是域,故 $\beta^{-1}\in F(B)$,从而 $\alpha\beta^{-1}\in F(A\cup B)\subset K$. 所以 K 是 $F(S)$ 的子域,即 K 是域.

注 1) 由该命题知,可以把添加无限集 S 于 F 所得的扩域 $F(S)$ 转化为添加有限个元于 F 所得的扩域的并.

2) 设 E 是域 F 的扩域,S_1,S_2 是 E 的子集,则 $F(S_1)\cup F(S_2)\subset F(S_1\cup S_2)$,但未必 $F(S_1)\cup F(S_2)=F(S_1\cup S_2)$.

事实上,$\forall \alpha\in F(S_1)\cup F(S_2)$,$\alpha\in F(S_1)$ 或 $\alpha\in F(S_2)$. 不妨设 $\alpha\in F(S_1)$,又 $F(S_1)\subset F(S_1)(S_2)=F(S_1\cup S_2)$,从而 $\alpha\in F(S_1\cup S_2)$. 所以 $F(S_1)\cup F(S_2)\subset F(S_1\cup S_2)$.

例 $\mathbb{C}$ 是 $\mathbb{Q}$ 的扩域,$\mathrm{i},\sqrt{2}\in\mathbb{C}$. $\mathrm{i}+\sqrt{2}\in\mathbb{Q}(\mathrm{i},\sqrt{2})$,但 $\mathrm{i}+\sqrt{2}\ \overline{\in}\ \mathbb{Q}(\mathrm{i})\cup\mathbb{Q}(\sqrt{2})$. 所以 $\mathbb{Q}(\mathrm{i})\cup\mathbb{Q}(\sqrt{2})\neq\mathbb{Q}(\mathrm{i},\sqrt{2})$. 因此子域的并未必是子域.

2. 令 E 是域 F 的一个扩域,而 $\alpha\in F$. 证明:α 是 F 上的一个代数元,并且 $F(\alpha)=F$.

证 因 $\alpha\in F$,故有 F 上非零多项式 $x-\alpha$,使 α 是 $x-\alpha$ 的根,所以 α 是 F 上代数元.

显然 $F\subset F(\alpha)$;反之,$F(\alpha)$ 是含 F 与 α 的 E 的最小子域,F 是含 F 与 α 的 E 的子域,从而 $F(\alpha)\subset F$. 所以 $F(\alpha)=F$.(还可如下证明,$\forall u\in F(\alpha)$,由第十六章,一,5,$u=\sum\limits_{i=0}^{n-1}a_i\alpha^i$,$a_i\in F$. 因 $\alpha\in F$,F 是域,故 $u\in F$,从而 $F(\alpha)\subset F$.)

注 1) 设 E 是域 F 的扩域,$\alpha\in E$,则

$$\alpha\in F \Leftrightarrow \alpha \text{ 是 } F \text{ 上一次代数元}.$$

事实上,(⇒) 因 α 在 F 上极小多项式是 $x-\alpha$.(⇐) 因 α 是 F 上一次代数元,故 α 在 F 上极小多项式为一次多项式 $p(x)=x-c$,且 $p(\alpha)=\alpha-c=0$,从而 $\alpha=c\in F$.

2) 设 E 是域 F 的扩域,$S\subset E$,则显然有

$$S\subset F \Leftrightarrow F(S)=F.$$

3. 令 $\mathbb{Q}$ 是有理数域. 复数 i 和 $\dfrac{2\mathrm{i}+1}{\mathrm{i}-1}$ 在 $\mathbb{Q}$ 上的极小多项式各是什么? $\mathbb{Q}(\mathrm{i})$ 与 $\mathbb{Q}\left(\dfrac{2\mathrm{i}+1}{\mathrm{i}-1}\right)$ 是否同构?

解　$p(x)=(x-\mathrm{i})(x+\mathrm{i})=x^2+1$ 在$\mathbf{Q}$上不可约，且 $p(\mathrm{i})=0$，从而 $p(x)$是 i 在$\mathbf{Q}$上极小多项式.

$\dfrac{2\mathrm{i}+1}{\mathrm{i}-1}=\dfrac{(1+2\mathrm{i})(-1-\mathrm{i})}{(-1+\mathrm{i})(-1-\mathrm{i})}=\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}$.　$q(x)=\left[x-\left(\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}\right)\right]\left[x-\left(\dfrac{1}{2}+\dfrac{3}{2}\mathrm{i}\right)\right]=x^2-x+\dfrac{5}{2}$在$\mathbf{Q}$上不可约，且 $q\left(\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}\right)=0$. 从而 $q(x)$是$\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}$ 在$\mathbf{Q}$上极小多项式.

$\mathbf{Q}(\mathrm{i})=\mathbf{Q}\left(\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}\right)$. 事实上，$\mathbf{Q}\subset\mathbf{Q}\left(\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}\right)$，$\mathrm{i}=-\dfrac{2}{3}\left(\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}\right)+\dfrac{1}{3}\in\mathbf{Q}\left(\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}\right)$，又$\mathbf{Q}(\mathrm{i})$是含$\mathbf{Q}$，i 的最小域，$\mathbf{Q}\left(\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}\right)$是含$\mathbf{Q}$，i 的域，从而$\mathbf{Q}(\mathrm{i})\subset\mathbf{Q}\left(\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}\right)$；反之，$\mathbf{Q}\subset\mathbf{Q}(\mathrm{i})$，$\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}\in\mathbf{Q}(\mathrm{i})$，从而$\mathbf{Q}\left(\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}\right)\subset\mathbf{Q}(\mathrm{i})$. 所以$\mathbf{Q}(\mathrm{i})=\mathbf{Q}\left(\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}\right)$，当然$\mathbf{Q}(\mathrm{i})\cong\mathbf{Q}\left(\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}\right)$.〔还可如下证明，$\forall\alpha\in\mathbf{Q}(\mathrm{i})$，因 $p(x)=x^2+1$ 是 i 在$\mathbf{Q}$上极小多项式，故由第十六章，一，5，$\alpha=a_0+a_1\mathrm{i}=\left(a_0+\dfrac{1}{3}a_1\right)+\left(-\dfrac{2}{3}a_1\right)\left(\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}\right)\in\mathbf{Q}\left(\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}\right)$，从而$\mathbf{Q}(\mathrm{i})\subset\mathbf{Q}\left(\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}\right)$；反之，$\forall\beta\in\mathbf{Q}\left(\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}\right)$，因 $q(x)=x^2-x+\dfrac{5}{2}$是$\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}$ 在$\mathbf{Q}$上极小多项式，故由第十六章，一，5，$\beta=b_0+b_1\left(\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}\right)=\left(b_0+\dfrac{1}{2}b_1\right)+\left(-\dfrac{3}{2}b_1\right)\mathrm{i}\in\mathbf{Q}(\mathrm{i})$，从而$\mathbf{Q}\left(\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}\right)\subset\mathbf{Q}(\mathrm{i})$. 所以$\mathbf{Q}(\mathrm{i})=\mathbf{Q}\left(\dfrac{1}{2}-\dfrac{3}{2}\mathrm{i}\right)$.〕

注　该例说明第十六章，一，7 中命题的逆命题不成立.

4. 详细证明：对于任一给定域 F 以及 F 上一元多项式环 $F[x]$的给定不可约多项式

$$p(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$$

总存在 F 的单代数扩域 $F(\alpha)$，其中 α 在域 F 上的极小多项式是 $p(x)$[①].

证　该命题要证明存在 F 的单代数扩域 $F(\alpha)$，使 α 在 F 上极小多项式是 $p(x)$.

由第十六章，一，4 中命题，单代数扩域$\cong F[x]/(p(x))$，从而就需要考虑 $F[x]/(p(x))$. $F[x]$是主理想环[②]，$(p(x))$是 $F[x]$的最大理想[③]，从而 $F[x]/(p(x))$是域[④]. 且自然同态ϕ：$f(x)\to\overline{f(x)}=f(x)+(p(x))$是环 $F[x]$到环 $F[x]/(p(x))$的同态满射[⑤]. 设 $F(\subset F[x]$在ϕ下的象是 $\overline{F}(\subset F[x]/(p(x))$，则 $\overline{F}$ 是 $F[x]/(p(x))$的子域[⑥]. 又 $\forall a\in F$，$\phi\big|_F$：$a\to\phi(a)=\bar{a}=a+(p(x))$是 F 到 $\overline{F}$ 的同态满射，且 $\forall a,b\in F$，若 $\bar{a}=\bar{b}$，则 $a-b\in(p(x))$，从而 $p(x)\big|a-b$. 因 $\deg p(x)=n>0$，故 $a-b=0$，即 $a=b$. 说明$\phi|_F$ 是 F 到 $\overline{F}$ 的单

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 158. 定理 3.

② 同上. 140. 定理 3. 139. 定理 1.

③ 同上. 136. 引理 2.

④ 同上. 118. 定理.

⑤ 同上. 114. 定理 1.

⑥ 同上. 116. 定理 3.

射. 所以 $F \overset{\phi|_F}{\cong} \overline{F}$.

由 $\overline{F}$ 是域 $F[x]/(p(x))$ 的子域, $F[x]/(p(x))-\overline{F}$ 与域 F 无共同元, $F\cong\overline{F}$, 由挖补定理, $\exists$ 域 K, 使得 $K \overset{\psi}{\cong} F[x]/(p(x))$, 其中, $\forall a\in F\subset K$, $\psi: a\to\phi(a)=\bar{a}\in\overline{F}$; $\forall\, \overline{f(x)}\in K-F$, $\psi: \overline{f(x)}\to\overline{f(x)}$, 且 F 是 K 的子域.

取 $x\in F[x]$, 则 $\phi(x)=\bar{x}=x+(p(x))\in F[x]/(p(x))$. 因 ψ 是满射, 故 $\exists\alpha\in K$, 使得 $\psi(\alpha)=\bar{x}$, 于是 α 是 F 上代数元. 事实上, 因 $p(\alpha)=\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_0\in K$, 故 $\psi(p(\alpha))=\psi(\alpha^n)+\psi(a_{n-1})\psi(\alpha^{n-1})+\cdots+\psi(a_0)=\bar{x}^n+\overline{a_{n-1}}\,\bar{x}^{n-1}+\cdots+\bar{a}_0$, 因 $p(x)\in F[x]$, 故 $\phi(p(x))=\phi(x^n+a_{n-1}x^{n-1}+\cdots+a_0)=\bar{x}^n+\overline{a_{n-1}}\,\bar{x}^{n-1}+\cdots+\bar{a}_0$. 从而 $\psi(p(\alpha))=\phi(p(x))=\overline{p(x)}=p(x)+(p(x))=\bar{0}=\psi(0)$, 因 ψ 是单射, 故 $p(\alpha)=0$. 于是 α 为 F 上代数元.

下面我们证明 $p(x)$ 是 α 在 F 上极小多项式. 事实上, $p(x)$ 是 F 上最高系数为 1 的不可约多项式且 $p(\alpha)=0$, 由第十六章, 一, 6, 2), (2) 知 $p(x)$ 是 α 在 F 上极小多项式.

另一证法, 由定义易证集 $A=\{f(x)\,|\,f(x)\in F[x], f(\alpha)=0\}$ 是 $F[x]$ 的一个理想. 设 $p_1(x)$ 是 α 在 F 上极小多项式. 因 $p_1(\alpha)=0$, 故 $p_1(x)\in A$. 因 A 是理想, 故 $(p_1(x))\subset A$; 反之, $\forall f(x)\in A$, 则 $f(\alpha)=0$. 又 $p_1(x)$ 是 α 在 F 上极小多项式, 从而由第十六章, 一, 6, 2), (1), $p_1(x)\,|\,f(x)$, 即 $\exists q(x)\in F[x]$, 使得 $f(x)=p_1(x)q(x)$, 因此 $f(x)\in(p_1(x))$, 于是 $A\subset(p_1(x))$. 所以 $A=(p_1(x))$. 因 $p(\alpha)=0$, 故 $p(x)\in A=(p_1(x))$, 从而 $p_1(x)\,|\,p(x)$. 因 $p(x)$ 在 F 上不可约, 又 $p_1(x)$ 是极小多项式, $p_1(x)\neq F[x]$ 的单位, 故 $p_1(x)$ 是 $p(x)$ 的相伴元, 因此 $p_1(x)=\varepsilon p(x)$, ε 是 F 的单位. 但 $p_1(x)$ 与 $p(x)$ 的最高系数都是 1, 从而 $\varepsilon=1$. 所以 $p(x)=p_1(x)$.

5. 证明: 对于上面题 4 证明中的 K, 有 $F[\alpha]=K$.

证 $\forall\,\overline{g(x)}\in F[x]/(p(x))$, 由 ϕ 是 $F[x]$ 到 $F[x]/(p(x))$ 的满射, $\exists\, g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_0\in F[x]$, 使得 $\phi(g(x))=\overline{g(x)}$. 又 $\phi(g(x))=\bar{b}_m\bar{x}^m+\overline{b_{m-1}}\,\bar{x}^{m-1}+\cdots+\bar{b}_0$, $\bar{b}_i\in\overline{F}$. 因 ϕ 是映射, 故 $\overline{g(x)}=\bar{b}_m\bar{x}^m+\overline{b_{m-1}}\,\bar{x}^{m-1}+\cdots+\bar{b}_0$, $\bar{b}_i\in\overline{F}$. 即 $F[x]/(p(x))$ 中的任一元都可表成如上形式.

$\forall\beta\in K$, 因 ψ 是 K 到 $F[x]/(p(x))$ 的映射, 故 $\exists\,\bar{b}^m\bar{x}^m+\overline{b_{m-1}}\,\bar{x}^{m-1}+\cdots+\bar{b}^0\in F[x]/(p(x))$, 使得 $\psi(\beta)=\bar{b}^m\bar{x}^m+\overline{b_{m-1}}\,\bar{x}^{m-1}+\cdots+\bar{b}^0$. 又 $\psi(b_m\alpha^m+b_{m-1}\alpha^{m-1}+\cdots+b_0)=\bar{b}^m\bar{x}^m+\overline{b_{m-1}}\,\bar{x}^{m-1}+\cdots+\bar{b}^0$, ψ 是单射, 从而 $\beta=b_m\alpha^m+b_{m-1}\alpha^{m-1}+\cdots+b_0\in F(\alpha)$, 即 $K\subset F(\alpha)$; 反之, 因 $F(\alpha)$ 是含 F,α 的最小域, K 是含 F,α 的域, 故 $F(\alpha)\subset K$. 所以 $F(\alpha)=K$.

注 1) 题 4 中命题说明域的单代数扩域必存在, 从而也称为单代数扩域的存在定理.

2) 该命题说明对于任一域 F 上不可约多项式 $p(x)$ (即任一域 F 上次数大于零的多项式), 都存在 F 的一个扩域 K, 使 $p(x)$ 在 K 中有一个根, 因此该命题也称为根的存在定理.

3) 该命题说明任一域 F 上最高系数为 1 的不可约多项式都是 F 上某代数元在 F 上

的极小多项式.

6. 令 E 是域 F 的一个代数扩域，而 α 是 E 上的一个代数元. 证明：α 是 F 上的一个代数元.

证　由 α 是 E 上代数元，$\exists E$ 上非零多项式 $f(x)=a_0+a_1x+\cdots a_nx^n$，使得 $f(\alpha)=0$. 由 E 是 F 的代数扩域，$a_i\in E$，a_i 是 F 上代数元. 则 $F(a_0,a_1,\cdots,a_n)$ 是 F 的有限扩域. 因 $\exists f(x)\in F(a_0,a_1,\cdots,a_n)[x]$，$f(x)\neq 0$，使得 $f(\alpha)=0$，故 α 是 $F(a_0,a_1,\cdots,a_n)$ 上代数元. 于是 $F(a_0,a_1,\cdots,a_n)(\alpha)$ 是 $F(a_0,a_1,\cdots,a_n)$ 的有限扩域，由第十六章，一，9，$F(a_0,a_1,\cdots,a_n,\alpha)$ 是 F 的有限扩域，由第十六章，一，10，$F(a_0,a_1,\cdots,a_n,\alpha)$ 是 F 的代数扩域. 所以 α 是 F 上代数元.

注　1)　若 E 是域 F 的扩域，α 是 F 上代数元，则显然 α 是 E 上代数元.

2)　若 E 是域 F 的扩域，α 是 E 上代数元，则 α 未必是 F 上代数元. 例，$\mathbb{R}$ 是 $\mathbb{Q}$ 的扩域，自然对数的底 e 是 $\mathbb{R}$ 上代数元，但 e 不是 $\mathbb{Q}$ 上代数元，因为 e 不可能是某个非零有理系数多项式的根.

3)　设 K 是域 E 的扩域，E 是域 F 的扩域，则

K 是 E 的代数扩域，E 是 F 的代数扩域 $\Leftrightarrow$ K 是 F 的代数扩域.

事实上，($\Rightarrow$)　$\forall\alpha\in K$，因 K 是 E 的代数扩域，故 α 是 E 上代数元. 又 E 是 F 的代数扩域，从而依该命题，α 是 F 上代数元. 由 α 在 K 中的任意性，K 是 F 的代数扩域. 说明代数扩域可以传递.

($\Leftarrow$)　$\forall\alpha\in E\subset K$，因 K 是 F 的代数扩域，故 α 是 F 上代数元，从而 E 是 F 的代数扩域.

$\forall\alpha\in K$，因 K 是 F 的代数扩域，故 α 是 F 上代数元. 因 E 是 F 的扩域，$E[x]\supset F[x]$，故 α 是 E 上代数元. 所以 K 是 E 的代数扩域.

4)　设 E 是 F 的有限扩域，若 α 是 E 上代数元，则 α 是 F 上代数元.

事实上，因有限扩域是代数扩域，故由该命题，α 是 F 上代数元.

另一证法，因 α 是 E 上代数元，故 $E(\alpha)$ 是 E 的单代数扩域. 从而 $E(\alpha)$ 是 E 的有限扩域. 因 E 是 F 的有限扩域，故由第十六章，一，9，$E(\alpha)$ 是 F 的有限扩域. 由第十六章，一，10，$E(\alpha)$ 是 F 的代数扩域. 所以 α 是 F 上代数元.

7. 令 F,I 和 E 是三个域，并且 $F\subset I\subset E$. 假定 $(I:F)=m$，而 E 的元 α 在 F 上的次数是 n，并且 $(m,n)=1$. 证明：α 在 I 上的次数也是 n.

证　已知 α 在 F 上的次数是 n，即 α 在 F 上极小多项式 $p(x)$ 的次数是 n. 因 I 是 F 的扩域，α 是 F 上代数元，故 α 是 I 上代数元. 设 α 在 I 上的次数为 s，即 α 在 I 上极小多项式 $q(x)$ 的次数为 s. 由第十六章，一，6，注 7)，在 $I[x]$ 中，$q(x)\mid p(x)$，从而 $s\leqslant n$. 下面再证明 $n\leqslant s$.
显然 $I(\alpha)\supset I\supset F$，$I(\alpha)\supset F(\alpha)\supset F$. 因单代数扩域 $I(\alpha)$ 是 I 的有限扩域，且 $(I(\alpha):I)=s$. 又 I 是 F 的有限扩域，依第十六章，一，9，$I(\alpha)$ 是 F 的有限扩域. 再由第十六章，一，9，2)，$I(\alpha)$ 是 $F(\alpha)$ 的有限扩域. 从而由第十六章，一，9，

$$(I(\alpha):F)=(I(\alpha):I)(I:F)=(I(\alpha):F(\alpha))(F(\alpha):F).$$

即 $sm=(I(\alpha):F(\alpha))n$，所以 $n\mid sm$. 因 $(m,n)=1$，故 $n\mid s$，即 $n\leqslant s$. 因此 $(I(\alpha):I)=s=n$.

8. 令域 F 的特征不是 2，E 是 F 的扩域，并且 $(E:F)=4$. 证明：存在一个满足条件 $F\subset$

$I\subset E$的 F 的二次扩域 I 的充分与必要条件是:$E=F(\alpha)$,而 α 在 F 上的极小多项式是 x^4+ax^2+b.

证一 ($\Leftarrow$) 已知 $E=F(\alpha)$,α 在 F 上极小多项式是 x^4+ax^2+b,$(F(\alpha):F)=4$,显然 $E\supset F(\alpha^2)\supset F$.下面证明$(F(\alpha^2):F)=2$.因 $F(\alpha)$是 F 的有限扩域,故由第十六章,一,9,2)及第十六章,一,9 中命题,

$$(F(\alpha):F)=(F(\alpha):F(\alpha^2))(F(\alpha^2):F)=4.$$

于是只需证明$(F(\alpha^2):F)\neq 1$ 且$(F(\alpha):F(\alpha^2))\neq 1$.$\alpha^2\overline{\in}F$,事实上,若 $\alpha^2\in F$,则$\exists c\in F$,使得 $\alpha^2=c$,从而 α 是 F 上二次多项式 x^2-c 的根,此与 α 在 F 上极小多项式是 4 次的矛盾.所以 $\alpha^2\overline{\in}F$,即 $F(\alpha^2)\neq F$.由第十六章,一,12,$(F(\alpha^2):F)\neq 1$.又 $\alpha\overline{\in}F(\alpha^2)$,事实上,若 $\alpha\in F(\alpha^2)$,则$\exists f(\alpha^2)\in F(\alpha^2)$,使得 $f(\alpha^2)=\alpha$.由第十五章,一,2,$\exists q(x^2)$,$ux^2+v\in F[x]$,使得

$$f(x^2)=(x^4+ax^2+b)q(x^2)+ux^2+v$$

即 $f(\alpha^2)=u\alpha^2+v$,从而 $u\alpha^2-\alpha+v=f(\alpha^2)-\alpha=0$,即 α 是 F 上二次多项式 ux^2-x+v 的根,同样与已知矛盾.所以 $\alpha\overline{\in}F(\alpha^2)$,与上同理,$(F(\alpha):F(\alpha^2))\neq 1$.因此$(F(\alpha^2):F)=2$.于是 $F(\alpha^2)$是一个满足条件 $F\subset F(\alpha^2)\subset E$ 的 F 的二次扩域.

($\Rightarrow$) 1) 首先证明,设 E 是域 I 的素数 p 次扩域,则$\forall\beta\in E$,$\beta\overline{\in}I$,都有 $E=I(\beta)$.

事实上,因$(E:I)=p\neq 1$,故由第十六章,一,12,$E\neq I$,从而在 E 中存在不属于 I 的元.$\forall\beta\in E$,$\beta\overline{\in}I$,由第十六章,一,9,2)及第十六章,一,9,

$$p=(E:I)=(E:I(\beta))(I(\beta):I).$$

因 $\beta\overline{\in}I$,故 $I(\beta)\neq I$,由第十六章,一,12,$(I(\beta):I)\neq 1$,但$(I(\beta):I)\mid p$,因此$(I(\beta):I)=p$.于是$(E:I(\beta))=1$.所以 $E=I(\beta)$.

2) 再证明,若 ch $I\neq 2$,$(E:I)=2$,则$\exists\alpha\in E$,使得 $E=I(\alpha)$且 α 在 I 上极小多项式呈形式 x^2-s.

事实上,因$(E:I)=2$,故由本题 1),$\exists\beta\in E$,$\beta\overline{\in}I$,使得 $E=I(\beta)$.因$(I(\beta):I)=2$,$\beta^2\in I(\beta)$,故由第十六章,一,5,$\beta^2=h\beta+k$,$h,k\in I$.因 ch $I\neq 2$,故 $2\cdot 1\neq 0$,其中 1 是域 I 的单位元.从而 $d=(2\cdot 1)^{-1}h\in I$,即 $h=(2\cdot 1)d$.于是 $\beta^2=(2\cdot 1)d\beta+k$,即 $\beta^2-2d\beta+d^2-d^2-k=0$,即$(\beta-d)^2-(d^2+k)=0$,令 $\alpha=\beta-d$,$s=d^2+k$,则 α 是 $x^2-s(\in I[x])$的根.又 $\alpha\in E$.因 $\beta\overline{\in}I$,$d\in I$,故 $\alpha=\beta-d\overline{\in}I$.由本题 1),$E=I(\alpha)$.又$(I(\alpha):I)=2$,从而 α 在 I 上极小多项式是 x^2-s.

3) 下面证明命题的必要性.

已知 ch $F\neq 2$,$F\subset I\subset E$.由第十一章,三,9,1),ch $I\neq 2$.而$(I:F)=2$,又$(E:F)=4$,由第十六章,一,9,2),E 是 I 的有限扩域,从而由第十六章,一,9,

$$4=(E:F)=(E:I)(I:F)=(E:I)2.$$

于是$(E:I)=2$.由本题 2),$\exists\alpha\in E$,$\alpha\overline{\in}I$,使得 $E=I(\alpha)$且 α 在 I 上极小多项式是 x^2-s,即 $s=\alpha^2\in I$.

① 若 $s\overline{\in}F$.而 $s\in I$,$(I:F)=2$,由本题 1),$I=F(s)$.因$(F(s):F)=2$,故 $s=\alpha^2$ 在 F 上极小多项式是 2 次的,设为 $g(x)=x^2+ax+b$,$a,b\in F$,从而 $g(s)=g(\alpha^2)=\alpha^4+a\alpha^2+b=0$,即 α 是 $x^4+ax^2+b(\in F[x])$的根.又

$$E=I(\alpha)=F(s)(\alpha)=F(\alpha^2)(\alpha)=F(\alpha).$$

已知$(F(\alpha):F)=4$,所以x^4+ax^2+b是α在F上极小多项式.命题得证.

② 若$s\in F$.因ch $F\neq 2$,$(I:F)=2$,故由本题2),$\exists\gamma\in I,\gamma\overline{\in}F$,使得$I=F(\gamma)$且$\gamma$在$F$上极小多项式是$x^2-t$,即$t=\gamma^2\in F$.注意到$\alpha^2=s\in F,\gamma^2=t\in F$,易验证$\alpha+\gamma$是$F$上多项式$x^4-(2s+2t)x^2+(s-t)^2$的根.又$s\neq t$,不然,若$s=t$,即$\alpha^2=\gamma^2,\alpha^2-\gamma^2=0$,即$(\alpha-\gamma)(\alpha+\gamma)=0$,因域$E$无零因子,故$\alpha=\gamma\in I$或$\alpha=-\gamma\in I$,此与$\alpha\overline{\in}I$矛盾,所以$s\neq t$,即$s-t\neq 0$,又ch $F\neq 2$,从而$2(s-t)\neq 0$,显然$2(t-s)\neq 0$.容易验证

$$\alpha=\left[2(t-s)\right]^{-1}\left[(\alpha+\gamma)^3-(t+3s)(\alpha+\gamma)\right],$$

$$\gamma=\left[2(s-t)\right]^{-1}\left[(\alpha+\gamma)^3-(s+3t)(\alpha+\gamma)\right].$$

因$t,s\in F$,故$\alpha,\gamma\in F(\alpha+\gamma)$.于是

$$E=I(\alpha)=F(\gamma)(\alpha)=F(\alpha,\gamma)=F(\alpha+\gamma).$$

由$(F(\alpha+\gamma):F)=4$,$x^4-(2s+2t)x^2+(s-t)^2$是$\alpha+\gamma$在F上极小多项式.命题得证.

证二 (⇐) 已知$E=F(\alpha)$,α在F上极小多项式是x^4+ax^2+b.显然$E\supset F(\alpha^2)\supset F$.因$g(x^2)=x^4+ax^2+b$在$F$上不可约,故$g(x)=x^2+ax+b$在$F$上也不可约.而$g(\alpha^2)=\alpha^4+a\alpha^2+b=0$,从而$g(x)$是$\alpha^2$在$F$上极小多项式,于是$(F(\alpha^2):F)=2$.所以取$I=F(\alpha^2)$即可.

(⇒) 已知ch $F\neq 2$,$F\subset I\subset E$,$(I:F)=2$,$(E:F)=4$.由证一,$(E:I)=2$.$\exists\alpha\in E$,$\alpha\overline{\in}I$,使得$E=I(\alpha)$,α在I上极小多项式是x^2-s,即$s=\alpha^2\in I$.$\exists\gamma\in I,\gamma\overline{\in}F$,使得$I=F(\gamma)$,$\gamma$在$F$上极小多项式是$x^2-t$,即$t=\gamma^2\in F$.因$s\in I=F(\gamma)$,$(F(\gamma):F)=2$,故由第十六章,一,5,$s=a_1+a_2\gamma$,$a_1,a_2\in F$.$E=I(\alpha)=F(\gamma)(\alpha)=F(\alpha,\gamma)$.

① 当$a_2\neq 0$时.

$$\begin{aligned}\alpha^4=s^2&=a_1^2+2a_1a_2\gamma+a_2^2\gamma^2+a_1^2-a_1^2\\&=2a_1(a_1+a_2\gamma)+a_2^2\gamma^2-a_1^2=2a_1s+a_2^2t-a_1^2\\&=2a_1\alpha^2+(a_2^2t-a_1^2).\end{aligned}$$

令$a=-2a_1$,$b=-(a_2^2t-a_1^2)$,则$a,b\in F$.且α是x^4+ax^2+b的一个根.又$a_2\gamma=s-a_1=\alpha^2-a_1$.因$a_2\neq 0$,故$\gamma=a_2^{-1}\alpha^2-a_2^{-1}a_1\in F(\alpha)$,从而$E=F(\alpha,\gamma)=F(\alpha)$.已知$(F(\alpha):F)=4$,于是$\alpha$在$F$上极小多项式是$x^4+ax^2+b$.命题得证.

② 当$a_2=0$时.

$\alpha+\gamma\neq 0$,否则,若$\alpha+\gamma=0$,则$\alpha=-\gamma\in I$,此与$\alpha\overline{\in}I$矛盾,所以$\alpha+\gamma\neq 0$.又ch $F\neq 2$,由第十一章,三,9,1),ch $E\neq 2$,从而$2(\alpha+\gamma)\neq 0$.又$\alpha^2=s=a_1$,$\gamma^2=t\in F$,因此$\exists[2(\alpha+\gamma)]^{-1}\in F(\alpha+\gamma)$,使得

$$\alpha=[2(\alpha+\gamma)]^{-1}\left[(\alpha+\gamma)^2+\alpha^2-\gamma^2\right]\in F(\alpha+\gamma),$$

$$\gamma=[2(\alpha+\gamma)]^{-1}\left[(\alpha+\gamma)^2-\alpha^2+\gamma^2\right]\in F(\alpha+\gamma).$$

从而$E=F(\alpha,\gamma)=F(\alpha+\gamma)$.又已知$(F(\alpha+\gamma):F)=4$,$\alpha+\gamma$是$F$上多项式$x^4-(2s+2t)x^2+(s+t)^2$的根(见证一),于是该多项式是$\alpha+\gamma$在$F$上极小多项式.命题得证.

证三 (⇐) 见证一.

(⇒) 由证一,$\exists\alpha\in E,\alpha\overline{\in}I$,使得$E=I(\alpha)$,$\alpha$在$I$上极小多项式是$x^2-s$,即$s=\alpha^2\in I$.

① 若$s\overline{\in}F$.见证一.

② 若 $s\in F$. 由证一，$\exists\gamma\in I$，$\gamma\overline{\in}F$，使得 $I=F(\gamma)$，γ 在 F 上极小多项式是 x^2-t，即 $t=\gamma^2\in F$. 考察

$$(\alpha+\alpha\gamma)^2=\alpha^2(1+\gamma)^2=\alpha^2(1+2\gamma+\gamma^2).$$

因 $\alpha^2=s$，$\gamma^2=t\in F$，$\gamma\in I$ 但 $\gamma\overline{\in}F$，即 $1+2\gamma+\gamma^2\overline{\in}F$，故 $(\alpha+\alpha\gamma)^2\overline{\in}F$，$(\alpha+\alpha\gamma)^2\in I$. 由证一（$\Rightarrow$）中 1），$I=F((\alpha+\alpha\gamma)^2)$. 已知 $(F(\alpha+\alpha\gamma)^2):F)=2$，从而 $(\alpha+\alpha\gamma)^2$ 在 F 上极小多项式是二次的，设为 $l(x)=x^2+\lambda x+\mu$，$\lambda,\mu\in F$. 于是 $l((\alpha+\alpha\gamma)^2)=(\alpha+\alpha\gamma)^4+\lambda(\alpha+\alpha\gamma)^2+\mu=0$，即 $\alpha+\alpha\gamma$ 是 $x^4+\lambda x+\mu(\in F[x])$ 的根.

因 $\alpha\overline{\in}I$，故 $\alpha\neq0$. 因 ch $E\neq2$，故 $2\alpha\neq0$. 又 $\alpha^2\gamma^2=st\in F$，从而

$$\alpha+\alpha\gamma=[2\alpha]^{-1}\left[(\alpha+\alpha\gamma)^2+\alpha^2-\alpha^2\gamma^2\right]\in F((\alpha+\alpha\gamma)^2,\alpha),$$

$\alpha+\alpha\gamma\neq0$. 不然，$\alpha=-\alpha\gamma$，因 $\alpha\neq0$，域 E 无零因子，故 $\gamma=-1\in F$，此与 $\gamma\overline{\in}F$ 矛盾. 所以 $\alpha+\alpha\gamma\neq0$. 因 ch $E\neq2$，故 $2(\alpha+\alpha\gamma)\neq0$. 又 $\alpha^2=s$，$\alpha^2\gamma^2\in F$，从而

$$\alpha=[2(\alpha+\alpha\gamma)]^{-1}\left[(\alpha+\alpha\gamma)^2+\alpha^2-\alpha^2\gamma^2\right]\in F(\alpha+\alpha\gamma).$$

于是

$$E=I(\alpha)=F((\alpha+\alpha\gamma)^2)(\alpha)=F((\alpha+\alpha\gamma)^2,\alpha)=F(\alpha+\alpha\gamma).$$

已知 $(F(\alpha+\alpha\gamma):F)=4$，所以 $\alpha+\alpha\gamma$ 在 F 上极小多项式是 $x^4+\lambda x+\mu$. 命题得证.

9. 令 E 是域 F 的一个有限扩域. 证明：总存在 E 的有限个元 $\alpha_1,\alpha_2,\cdots,\alpha_m$，使 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_m)$.

证 因 E 是域 F 的有限扩域，故 E 作为 F 上的向量空间有维数 m，从而 E 在 F 上有基 $\alpha_1,\alpha_2,\cdots,\alpha_m$. 于是 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_m)$. 事实上，$\forall\alpha\in E$，$\exists a_1,a_2,\cdots,a_m\in F$，使得 $\alpha=\sum_{i=1}^{m}a_i\alpha_i\in F(\alpha_1,\alpha_2,\cdots,\alpha_m)$，因此 $E\subset F(\alpha_1,\alpha_2,\cdots,\alpha_m)$；反之，$F(\alpha_1,\alpha_2,\cdots,\alpha_m)$ 是包含 $F,\alpha_1,\alpha_2,\cdots,\alpha_m$ 的最小域，E 是包含 $F,\alpha_1,\alpha_2,\cdots,\alpha_m$ 的域，因此 $F(\alpha_1,\alpha_2,\cdots,\alpha_m)\subset E$. 所以 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_m)$.

注 1） 我们有：E 是域 F 的有限扩域 $\Leftrightarrow$ $\exists$ 域 F 上有限个代数元 $\alpha_1,\alpha_2,\cdots,\alpha_m\in E$，使得

$$E=F(\alpha_1,\alpha_2,\cdots,\alpha_m).$$

2） 在域 F 上添加有限个代数元所得的扩域和域 F 的有限扩域这两个概念是一致的. 但在 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_m)$ 中添加的代数元的个数 m 与扩域次数 $(E:F)$ 未必相等. 即 $(F(\alpha_1,\alpha_2,\cdots,\alpha_m):F)$ 未必 $=m$. 例如 $(\mathbf{R}(\mathrm{i}):\mathbf{R})=2$.

3） 在域 F 上添加有限个元所得的扩域和域 F 的有限扩域这两个概念却不一致. 见第十六章，一，10. 即该命题的逆命题不成立.

10. 令 $\mathbf{Q}$ 是有理数域. 看添加复数于 $\mathbf{Q}$ 所得扩域：$E_1=\mathbf{Q}(2^{\frac{1}{3}},2^{\frac{1}{3}}\mathrm{i})$，$E_2=\mathbf{Q}(2^{\frac{1}{3}},2^{\frac{1}{3}}\omega\mathrm{i})$，$\omega=\dfrac{-1+\sqrt{3}\,\mathrm{i}}{2}$，$\omega^3=1$. 证明：$(E_1:\mathbf{Q}(2^{\frac{1}{3}}))=2$，$(E_1:\mathbf{Q})=6$，$(E_2:\mathbf{Q}(2^{\frac{1}{3}}))=4$，$(E_2:\mathbf{Q})=12$.

证一 $2^{\frac{1}{3}}\mathrm{i}$ 是 $\mathbf{Q}(2^{\frac{1}{3}})$ 上多项式 $p(x)=(x-2^{\frac{1}{3}}\mathrm{i})(x+2^{\frac{1}{3}}\mathrm{i})=x^2+2^{\frac{2}{3}}$ 的根. 又 $p(x)$ 在 $\mathbf{Q}(2^{\frac{1}{3}})$ 上不可约. 否则，$p(x)$ 在 $\mathbf{Q}(2^{\frac{1}{3}})$ 中有根. 因 $2^{\frac{1}{3}}$ 在 $\mathbf{Q}$ 上极小多项式是 x^3-2，故可设 $a+b2^{\frac{1}{3}}+c2^{\frac{2}{3}}(\in\mathbf{Q}(2^{\frac{1}{3}}))$ 是 $p(x)$ 的根，即 $(a+b2^{\frac{1}{3}}+c2^{\frac{2}{3}})^2+2^{\frac{2}{3}}=0$，即 $a^2+4bc+(b^2+2ac+1)2^{\frac{2}{3}}+$

$(2c^2+2ab)2^{\frac{1}{3}}=0$，即 $a^2+4bc=0, b^2+2ac+1=0, c^2+ab=0$. 从而 $a^2b^2=c^4, (-4bc)b^2=c^4$，即 $-4b^3c=c^4$. $c\neq 0$，否则，若 $c=0$，则 $b^2=-1$，矛盾. 于是 $c\neq 0$，因此 $-4b^3=c^3$，即 $\frac{b^3}{c^3}=\left(\frac{b}{c}\right)^3=-\frac{1}{4}$，矛盾. 所以 $p(x)$ 在 $\mathbf{Q}(2^{\frac{1}{3}})$ 上不可约. 从而 $p(x)$ 是 $2^{\frac{1}{3}}\mathrm{i}$ 在 $\mathbf{Q}(2^{\frac{1}{3}})$ 上极小多项式，即

$$(E_1:\mathbf{Q}(2^{\frac{1}{3}}))=(\mathbf{Q}(2^{\frac{1}{3}})(2^{\frac{1}{3}}\mathrm{i}):\mathbf{Q}(2^{\frac{1}{3}}))=2.$$

容易验证 $\alpha_1=1, \alpha_2=2^{\frac{1}{3}}\omega\mathrm{i}, \alpha_3=(2^{\frac{1}{3}}\omega\mathrm{i})^2, \alpha_4=(2^{\frac{1}{3}}\omega\mathrm{i})^3$ 对于 $\mathbf{Q}(2^{\frac{1}{3}})$ 来说线性无关. 而

$$(2^{\frac{1}{3}}\omega\mathrm{i})^4=2^{\frac{4}{3}}\omega=-2^{\frac{4}{3}}\alpha_1+0\alpha_2+2^{\frac{2}{3}}\alpha_3+0\alpha_4.$$

即 $\alpha_1,\alpha_2,\alpha_3,\alpha_4,(2^{\frac{1}{3}}\omega\mathrm{i})^4$ 对于 $\mathbf{Q}(2^{\frac{1}{3}})$ 来说线性相关. 因此 $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ 是 E_2 在 $\mathbf{Q}(2^{\frac{1}{3}})$ 上的一个基，于是 $(E_2:\mathbf{Q}(2^{\frac{1}{3}}))=4$.（实际上，$x^4-2^{\frac{2}{3}}x^2+2^{\frac{4}{3}}$ 是 $2^{\frac{1}{3}}\omega\mathrm{i}$ 在 $\mathbf{Q}(2^{\frac{1}{3}})$ 上极小多项式.）

由第十五章，四，13，艾森斯坦因不可约性判别准则，x^3-2 在 $\mathbf{Q}$ 上不可约，从而 $2^{\frac{1}{3}}$ 在 $\mathbf{Q}$ 上极小多项式是 x^3-2，于是 $(\mathbf{Q}(2^{\frac{1}{3}}):\mathbf{Q})=3$. 所以

$$(E_1:\mathbf{Q})=(E_1:\mathbf{Q}(2^{\frac{1}{3}}))(\mathbf{Q}(2^{\frac{1}{3}}):\mathbf{Q})=2\cdot 3=6.$$

$$(E_2:\mathbf{Q})=(E_2:\mathbf{Q}(2^{\frac{1}{3}}))(\mathbf{Q}(2^{\frac{1}{3}}):\mathbf{Q})=4\cdot 3=12.$$

证二　因 $\mathrm{i}=2^{-\frac{1}{3}}\cdot 2^{\frac{1}{3}}\mathrm{i}\in\mathbf{Q}(2^{\frac{1}{3}},2^{\frac{1}{3}}\mathrm{i})=E_1$，故

$$E_1=\mathbf{Q}(2^{\frac{1}{3}},2^{\frac{1}{3}}\mathrm{i})=\mathbf{Q}(2^{\frac{1}{3}},\mathrm{i})\supset\mathbf{Q}(2^{\frac{1}{3}})\supset\mathbf{Q}.$$

因 x^2+1 是 i 在 $\mathbf{Q}(2^{\frac{1}{3}})$ 上极小多项式，故

$$(E_1:\mathbf{Q}(2^{\frac{1}{3}}))=(\mathbf{Q}(2^{\frac{1}{3}})(\mathrm{i}):\mathbf{Q}(2^{\frac{1}{3}}))=2.$$

因 $2^{\frac{1}{3}}$ 在 $\mathbf{Q}$ 上极小多项式是 x^3-2，故 $(\mathbf{Q}(2^{\frac{1}{3}}):\mathbf{Q})=3$，从而

$$(E_1:\mathbf{Q})=(E_1:\mathbf{Q}(2^{\frac{1}{3}}))(\mathbf{Q}(2^{\frac{1}{3}}):\mathbf{Q})=2\cdot 3=6.$$

因 $\mathrm{i}=-(\omega\mathrm{i})^3=-\frac{1}{2}(2^{\frac{1}{3}}\omega\mathrm{i})^3\in\mathbf{Q}(2^{\frac{1}{3}},2^{\frac{1}{3}}\omega\mathrm{i}), \sqrt{3}=-2\omega\mathrm{i}-\mathrm{i}=-2^{\frac{2}{3}}(2^{\frac{1}{3}}\omega\mathrm{i})-\mathrm{i}\in\mathbf{Q}(2^{\frac{1}{3}},2^{\frac{1}{3}}\omega\mathrm{i})$，故

$$E_2=\mathbf{Q}(2^{\frac{1}{3}},2^{\frac{1}{3}}\omega\mathrm{i})=\mathbf{Q}(2^{\frac{1}{3}},\sqrt{3},\mathrm{i})\supset\mathbf{Q}(2^{\frac{1}{3}},\sqrt{3})\supset\mathbf{Q}(2^{\frac{1}{3}})\supset\mathbf{Q}.$$

因 i 在 $\mathbf{Q}(2^{\frac{1}{3}},\sqrt{3})$ 上极小多项式是 x^2+1，故

$$(E_2:\mathbf{Q}(2^{\frac{1}{3}},\sqrt{3}))=(\mathbf{Q}(2^{\frac{1}{3}},\sqrt{3})(\mathrm{i}):\mathbf{Q}(2^{\frac{1}{3}},\sqrt{3}))=2.$$

x^2-3 在 $\mathbf{Q}(2^{\frac{1}{3}})$ 上不可约. 否则，x^2-3 在 $\mathbf{Q}(2^{\frac{1}{3}})$ 中有根. 因 $2^{\frac{1}{3}}$ 在 $\mathbf{Q}$ 上极小多项式是 x^3-2，故可设 x^2-3 在 $\mathbf{Q}(2^{\frac{1}{3}})$ 中的根为 $a_0+a_12^{\frac{1}{3}}+a_22^{\frac{2}{3}}$，从而 $(a_0+a_12^{\frac{1}{3}}+a_22^{\frac{2}{3}})^2-3=0$，即 $(a_0^2+4a_1a_2-3)+(a_1^2+2a_0a_2)2^{\frac{2}{3}}+(2a_2^2+2a_0a_1)2^{\frac{1}{3}}=0$，即 $a_0^2+4a_1a_2=3, a_1^2+2a_0a_2=0, a_2^2+a_0a_1=0$. 于是 $a_0^2a_1^2=a_2^4, -a_0^2(2a_0a_2)=a_2^4$，即 $-2a_0^3a_2=a_2^4$. 因 $a_2\neq 0$，否则，$a_0^2=3$，矛盾，故 $-2a_0^3=a_2^3$，即 $\left(\frac{a_0}{a_2}\right)^3=-\frac{1}{2}$，矛盾. 所以 x^2-3 在 $\mathbf{Q}(2^{\frac{1}{3}})$ 上不可约. 因此 $\sqrt{3}$ 在 $\mathbf{Q}(2^{\frac{1}{3}})$ 上极小多项式是 x^2-3，即 $(\mathbf{Q}(2^{\frac{1}{3}})(\sqrt{3}):\mathbf{Q}(2^{\frac{1}{3}}))=2$. 于是

$$(E_2:\mathbf{Q}(2^{\frac{1}{3}}))=(E_2:\mathbf{Q}(2^{\frac{1}{3}},\sqrt{3}))(\mathbf{Q}(2^{\frac{1}{3}})(\sqrt{3}):\mathbf{Q}(2^{\frac{1}{3}}))=2\cdot 2=4.$$

$$(E_2:\mathbf{Q})=(E_2:\mathbf{Q}(2^{\frac{1}{3}}))(\mathbf{Q}(2^{\frac{1}{3}}):\mathbf{Q})=4\cdot 3=12.$$

注 1) 还可如下证明$(E_2:\mathbb{Q}(2^{\frac{1}{3}}))=4$.

因$\omega \mathrm{i}=2^{-\frac{1}{3}}(2^{\frac{1}{3}}\omega \mathrm{i})\in \mathbb{Q}(2^{\frac{1}{3}},2^{\frac{1}{3}}\omega \mathrm{i})$,故$E_2=\mathbb{Q}(2^{\frac{1}{3}},2^{\frac{1}{3}}\omega \mathrm{i})=\mathbb{Q}(2^{\frac{1}{3}},\omega \mathrm{i})$. $\omega \mathrm{i}=-\frac{\sqrt{3}}{2}-\frac{\mathrm{i}}{2}$.

$$\left[x-\left(-\frac{\sqrt{3}}{2}-\frac{\mathrm{i}}{2}\right)\right]\left[x-\left(-\frac{\sqrt{3}}{2}+\frac{\mathrm{i}}{2}\right)\right]\left[x-\left(\frac{\sqrt{3}}{2}-\frac{\mathrm{i}}{2}\right)\right]\left[x-\left(\frac{\sqrt{3}}{2}+\frac{\mathrm{i}}{2}\right)\right]$$

$$=\left[\left(x+\frac{\sqrt{3}}{2}\right)^2-\left(\frac{\mathrm{i}}{2}\right)^2\right]\left[\left(x-\frac{\sqrt{3}}{2}\right)^2-\left(\frac{\mathrm{i}}{2}\right)^2\right]=(x^2+\sqrt{3}x+1)(x^2-\sqrt{3}x+1)$$

$$=(x^2+1)^2-(\sqrt{3}x)^2=x^4-x^2+1.$$

从而$\omega \mathrm{i}$是$\mathbb{Q}(2^{\frac{1}{3}})$上多项式$x^4-x^2+1$的根,又$x^4-x^2+1$在$\mathbb{Q}(2^{\frac{1}{3}})$上不可约.因此$x^4-x^2+1$是$\omega \mathrm{i}$在$\mathbb{Q}(2^{\frac{1}{3}})$上极小多项式.所以$(E_2:\mathbb{Q}(2^{\frac{1}{3}}))=(\mathbb{Q}(2^{\frac{1}{3}})(\omega \mathrm{i}):\mathbb{Q}(2^{\frac{1}{3}}))=4$.

2) 证明$(E_2:\mathbb{Q}(2^{\frac{1}{3}}))=4$的又一方法.

因$\mathrm{i}\in\mathbb{Q}(2^{\frac{1}{3}},2^{\frac{1}{3}}\omega \mathrm{i})$(见证二),$\omega=2^{-\frac{1}{3}}\mathrm{i}^{-1}(2^{\frac{1}{3}}\omega \mathrm{i})\in\mathbb{Q}(2^{\frac{1}{3}},2^{\frac{1}{3}}\omega \mathrm{i})$,故$E_2=\mathbb{Q}(2^{\frac{1}{3}},2^{\frac{1}{3}}\omega \mathrm{i})=\mathbb{Q}(2^{\frac{1}{3}},\omega,\mathrm{i})$.因$\mathrm{i}$在$\mathbb{Q}(2^{\frac{1}{3}},\omega)$上极小多项式是$x^2+1$,故$(E_2:\mathbb{Q}(2^{\frac{1}{3}},\omega)=(\mathbb{Q}(2^{\frac{1}{3}},\omega)(\mathrm{i}):\mathbb{Q}(2^{\frac{1}{3}},\omega))=2$.因$\omega$在$\mathbb{Q}(2^{\frac{1}{3}})$上极小多项式是$x^2+x+1$,故$(\mathbb{Q}(2^{\frac{1}{3}})(\omega):\mathbb{Q}(2^{\frac{1}{3}}))=2$.所以

$$(E_2:\mathbb{Q}(2^{\frac{1}{3}}))=(E_2:\mathbb{Q}(2^{\frac{1}{3}},\omega))(\mathbb{Q}(2^{\frac{1}{3}})(\omega):\mathbb{Q}(2^{\frac{1}{3}}))=2\cdot 2=4.$$

三、讲与练

1. 判断下面各命题是否正确.

1) 4个元作成的域$F=\{0,1,a,a+1\}$(第十章,二,6)是素域.

2) 设$F(\alpha)$,$F(\beta)$是域F的单扩域.若$\alpha\in F(\beta)$,$\beta\in F(\alpha)$,则$F(\alpha)=F(\beta)$.

3) 设$p(x)$是域F上不可约多项式,则$p(x)$也是单扩域$F(\alpha)$上不可约多项式.

4) 设E与E'都是域F的扩域,且$E\cong E'$,则$E=E'$.

5) 设$F(\alpha)$,$F(\beta)$是域F的单代数扩域.若ϕ是$F(\alpha)$与$F(\beta)$间的同构映射,则α在ϕ下的象必为β.

6) 设E是域F的扩域,$\alpha\in E$.则

α是F上代数元$\Leftrightarrow \exists f(x)\in F[x]$, $f(x)\neq 0$,使得$f(\alpha)=0$

$\Leftrightarrow F(\alpha)\cong F[x]/(p(x))$,$p(x)$是$\alpha$在$F$上极小多项式

$\Leftrightarrow F[\alpha]=F(\alpha)$是域

$\Leftrightarrow F(\alpha)=\{f(\alpha)\mid f(x)\in F[x]\}$是$F$的有限扩域.

7) 设E是域F的扩域,$\alpha\in E$.则α是F上超越元$\Leftrightarrow \forall f(x)\in F[x]$,若$f(\alpha)=0$,则$f(x)=0$

$\Leftrightarrow \forall f(x)(\neq 0)\in F[x]$,$f(\alpha)\neq 0$

$\Leftrightarrow \alpha$是F上未定元

$\Leftrightarrow n$是任意非负整数,$1,\alpha,\alpha^2,\cdots,\alpha^n$对于$F$来说线性无关.

8) 设x是域F上未定元,$f(x)$,$g(x)\in F[x]$.若α是F上代数元,$f(\alpha)=g(\alpha)$,则$f(x)=g(x)$.

9)　设 x 是域 F 上未定元，$f(x),g(x)\in F[x]$. 若 α 是 F 上超越元，$f(\alpha)=g(\alpha)$，则 $f(x)=g(x)$.

10)　设 E 是域 F 的扩域. 若 α 是 E 上也是 F 上的代数元，则 α 在 E 上与在 F 上的极小多项式相同.

11)　域 E 是自身的代数扩域.

12)　$\mathbf{Q}(\sqrt{2},\sqrt[3]{3},\sqrt[5]{5},\sqrt[7]{7},\cdots,\sqrt[p]{p},\cdots)$（$p$ 是素数）是 $\mathbf{Q}$ 的代数扩域.

13)　设 E 是域 F 的扩域，则

$$E\text{ 是 }F\text{ 的有限扩域}\Leftrightarrow E\text{ 是 }F\text{ 上的有限维空间}.$$

14)　设 E 是域 F 的扩域，则 $(E:F)\neq 0$.

15)　若 E 是域 F 的有限扩域，则 E 只含有限个元.

16)　设 E 是域 F 的扩域，E 含有限个元，则 E 是 F 的有限扩域.

17)　设 E 是域 I 的扩域，I 是域 F 的扩域，E 是 F 的有限扩域. 若 $(E:F)=$ 素数 p，则 $I=E$ 或 $I=F$.

18)　设 E 是域 I 的扩域，I 是域 F 的扩域.

①　若 $(E:F)=(I:F)$，则 $E=I$.

②　若 $(E:I)=(E:F)$，则 $I=F$.

19)　设 F 是域，$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$，且 α_i 是 $F(\alpha_1,\alpha_2,\cdots,\alpha_{i-1})$ 上代数元，$i=2,3,\cdots,n$. α_1 是 F 上代数元，则 E 是 F 的有限扩域.

20)　设 E 是域 F 的扩域，$\alpha(\in E)$ 是 F 上代数元，$\beta\in F(\alpha)$，则 β 在 F 上的次数是 α 在 F 上的次数的因子.

21)　$\mathbf{Q}(\pi)$ 是域 $\mathbf{Q}(\pi^6)$ 的单代数扩域.

解　1)　不正确. 由第十六章，一，1，注 1)知，含有限个元的素域必有素数个元. 实际上，F 有真子域 $\{0,1\}$.

2)　正确. 事实上，由 $\alpha\in F(\beta)$，有 $F(\alpha)\subset F(\beta)$；由 $\beta\in F(\alpha)$，有 $F(\beta)\subset F(\alpha)$. 所以 $F(\alpha)=F(\beta)$.

3)　不正确. 例，x^2-2 在 $\mathbf{Q}$ 上不可约，但 x^2-2 在 $\mathbf{Q}(\sqrt{2})$ 上可约，因 $x^2-2=(x+\sqrt{2})(x-\sqrt{2})$.

4)　不正确. 例，$\sqrt[3]{2}$ 与 $\sqrt[3]{2}\omega$ 在 $\mathbf{Q}$ 上有相同的极小多项式 x^3-2. 由第十六章，一，7，$\mathbf{Q}(\sqrt[3]{2})\cong\mathbf{Q}(\sqrt[3]{2}\omega)$. 因 $\sqrt[3]{2}\omega\,\overline{\in}\,\mathbf{Q}(\sqrt[3]{2})$，故 $\mathbf{Q}(\sqrt[3]{2})\neq\mathbf{Q}(\sqrt[3]{2}\omega)$.

5)　不正确. 例，$\mathbf{Q}(1)$，$\mathbf{Q}(2)$ 是 $\mathbf{Q}$ 的单代数扩域. $\phi:a\to a$ 是 $\mathbf{Q}(1)=\mathbf{Q}$ 与 $\mathbf{Q}(2)=\mathbf{Q}$ 间的同构映射. 但 1 在 ϕ 下的象是 $1\neq 2$.

6)　正确. 由定义，第十六章，一，4，第十六章，一，10 可知.

7)　正确. 由定义可知.

8)　不正确. 因 α 是 F 上代数元，故 $\exists\, h(x)(\neq 0)\in F[x]$，使得 $h(\alpha)=0$，从而 $\forall\, k(x)\in F[x]$，有 $k(\alpha)+h(\alpha)=k(\alpha)$. 但 $k(x)+h(x)\neq k(x)$.

9)　正确. 事实上，假设 $f(x)\neq g(x)$，则 $s(x)=f(x)-g(x)\neq 0$，而 $s(\alpha)=f(\alpha)-g(\alpha)=0$，从而 α 是 F 上非零多项式 $s(x)$ 的根，于是 α 是 F 上代数元. 矛盾.

10)　不正确. 例，$\mathbf{R}$ 是 $\mathbf{Q}$ 的扩域. $\sqrt{2}$ 是 $\mathbf{R}$ 上也是 $\mathbf{Q}$ 上的代数元. $\sqrt{2}$ 在 $\mathbf{R}$ 上极小多项式是 $x-\sqrt{2}$，但 $\sqrt{2}$ 在 $\mathbf{Q}$ 上极小多项式是 x^2-2（参看第十六章，一，6，注 7)）.

11） 正确.事实上,E 是 E 的扩域.由第十六章,二,2,$\forall\alpha\in E$,α 是 E 上代数元,从而 E 是 E 的代数扩域.

12） 正确.设 p 是任一素数.因 $\sqrt[p]{p}$ 是 $\mathbb{Q}$ 上非零多项式 x^p-p 的根,故 $\sqrt[p]{p}$ 是 $\mathbb{Q}$ 上代数元.由第十六章,一,11,E 是 $\mathbb{Q}$ 的代数扩域.

13） 正确.由定义知.

14） 正确.因域 $E\neq\{0\}$,故 E 不是 F 上的零维向量空间,从而 $(E:F)\neq 0$.

15） 不正确.例,$1,\mathrm{i}(\in\mathbb{C})$ 对于 $\mathbb{R}$ 来说线性无关.$\forall\alpha\in\mathbb{C}$,$\alpha=a1+b\mathrm{i}$,$a,b\in\mathbb{R}$.从而 $1,\mathrm{i}$ 是 $\mathbb{C}$ 在 $\mathbb{R}$ 上的一个基.于是 $\mathbb{C}$ 是 $\mathbb{R}$ 上 2 维向量空间,所以 $\mathbb{C}$ 是 $\mathbb{R}$ 的有限扩域.但 $\mathbb{C}$ 含无限多个元.

16） 正确.事实上,假设 E 是 F 的无限扩域,则 E 是 F 上无限维空间,即 E 含有任意多个对于 F 来说的线性无关的元,从而 E 含无限多个元,矛盾.

17） 正确.由第十六章,一,9,2)及第十六章,一,9 中命题,$(E:F)=(E:I)(I:F)=p$.因 p 是素数,故 $(E:I)=1$ 或 $(I:F)=1$.由第十六章,一,12,$I=E$ 或 $I=F$.

注 依该命题,可直接证明第十一章,二,3.

18） 正确.事实上,① 因 E 是 F 的有限扩域,故由第十六章,一,9,2),E 是 I 的有限扩域.由第十六章,一,9,$(E:F)=(E:I)(I:F)$.今 $(E:F)=(I:F)\neq 0$,从而 $(E:I)=1$.已知 $E\supset I$,由第十六章,一,12,$E=I$.

另一证法,设 $(E:F)=(I:F)=n$,则 $\exists\,\alpha_1,\alpha_2,\cdots,\alpha_n\in I$,$\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 I 在 F 上的一个基.因 $I\subset E$,$(E:F)=n$,故 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 也是 E 在 F 上的一个基.从而 $\forall\alpha\in E$,有 $\alpha=\sum_1^n a_i\alpha_i$,$a_i\in F$,于是 $\alpha\in I$,即 $E\subset I$.所以 $E=I$.

② 与①类似地可证.

19） 正确.事实上,因 α_i 是 $F(\alpha_1,\alpha_2,\cdots,\alpha_{i-1})$ 上代数元,故单代数扩域 $F(\alpha_1,\alpha_2,\cdots,\alpha_{i-1})(\alpha_i)$ 是 $F(\alpha_1,\alpha_2,\cdots,\alpha_{i-1})$ 的有限扩域,$i=2,3,\cdots,n$.且 $F(\alpha_1)$ 是 F 的有限扩域.则

$$(E:F)=\big(E:F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})\big)\big(F(\alpha_1,\alpha_2,\cdots,\alpha_{n-2})(\alpha_{n-1}):F(\alpha_1,\alpha_2,\cdots,\alpha_{n-2})\big)\cdots(F(\alpha_1):F).$$

所以 E 是 F 的有限扩域.

20） 正确.事实上,因 $\beta\in F(\alpha)$,故 $F(\beta)$ 是 $F(\alpha)$ 的子域.且 $F(\alpha)$ 是 F 的有限扩域.由第十六章,一,9,2)及第十六章,一,9,$(F(\alpha):F)=(F(\alpha):F(\beta))(F(\beta):F)$.
所以 $(F(\beta):F)\mid(F(\alpha):F)$.

注 利用该命题可证明某些多项式不可约.例,x^3-2 在 $\mathbb{Q}(\sqrt{2})$ 上不可约.否则 x^3-2 在 $\mathbb{Q}(\sqrt{2})$ 中有根 β.从而 β 是 $\mathbb{Q}$ 上代数元,且 x^3-2 是 β 在 $\mathbb{Q}$ 上极小多项式,即 $(\mathbb{Q}\beta:\mathbb{Q})=3$.$\sqrt{2}(\in\mathbb{Q}(\sqrt{2}))$ 是 $\mathbb{Q}$ 上二次代数元.由该命题,$3\mid 2$,矛盾.所以 x^3-2 在 $\mathbb{Q}(\sqrt{2})$ 中没有根,即 x^3-2 在 $\mathbb{Q}(\sqrt{2})$ 上不可约.

21） 正确.事实上,因 π 是 $\mathbb{Q}(\pi^6)$ 上非零多项式 $x^6-\pi^6$ 的一个根,故 π 是 $\mathbb{Q}(\pi^6)$ 上代数元,从而 $\mathbb{Q}(\pi^6)(\pi)$ 是 $\mathbb{Q}(\pi^6)$ 的单代数扩域.又 $\mathbb{Q}(\pi^6)(\pi)=\mathbb{Q}(\pi)$.所以 $\mathbb{Q}(\pi)$ 是 $\mathbb{Q}(\pi_6)$ 的单代数扩域.

2. 判断下列各元 α 是否为域 F 上代数元.若是,求出 α 在 F 上极小多项式,$(F(\alpha):F)=?$

$F(\alpha)$与哪个剩余类环同构？$F(\alpha)$的元都可唯一表成什么形式？

1)　$\alpha=\beta+a$，其中β是域F上超越元，$a\in F$.

2)　π是$\mathbf{Q}$上超越元，$-\pi+2$是$\mathbf{Q}$上超越元，α是这两个$\mathbf{Q}$上超越元的和，$F=\mathbf{Q}$.

3)　$\alpha=\beta^2$，其中β是域F上超越元.

4)　$\alpha=\mathrm{i}$，$F=\mathbb{Z}_7$.

5)　$\alpha=a+b\mathrm{i}$ $(a,b\in\mathbf{Q},b\neq0)$，$F=\mathbf{Q}$.

6)　$\alpha=a+b\mathrm{i}$ $(a,b\in\mathbf{R},b\neq0)$，$F=\mathbf{R}$.

7)　$\alpha=\cos\dfrac{2\pi}{p}+\mathrm{i}\sin\dfrac{2\pi}{p}=\mathrm{e}^{\frac{2\pi}{p}\mathrm{i}}$，其中$p$是素数，$F=\mathbf{Q}$.

8)　$\alpha=\cos\dfrac{2\pi}{12}+\mathrm{i}\sin\dfrac{2\pi}{12}=\mathrm{e}^{\frac{2\pi}{12}\mathrm{i}}$，$F=\mathbf{Q}$.

9)　$\alpha=\sqrt[3]{2}\varepsilon$，其中$\varepsilon=\dfrac{1}{2}+\dfrac{\sqrt{3}}{2}\mathrm{i}$，$F=\mathbf{Q}$.

10)　$\alpha=\sqrt[n]{p}$，其中p是素数，n是>1的整数. $F=\mathbf{Q}$.

11)　$\alpha=1+\sqrt{2}$，$F=\mathbf{Q}$.

12)　$\alpha=\sqrt{1+\sqrt{3}}$，$F=\mathbf{Q}$.

解　1)　$\alpha=\beta+a$不是F上代数元. 事实上，假设α是F上代数元，又因$a\in F$，故由第十六章，二，2，a是F上代数元. 由第十六章，一，11，$\alpha-a=\beta$也是F上代数元，矛盾.

2)　$\alpha=\pi+(-\pi+2)=2$是$\mathbf{Q}$上代数元. 2在$\mathbf{Q}$上极小多项式是$x-2$. $(\mathbf{Q}(2):\mathbf{Q})=1$. $\mathbf{Q}(2)\cong\mathbf{Q}[x]/(x-2)$. $\mathbf{Q}(2)=\left\{a\,\middle|\,a\in\mathbf{Q}\right\}$.

注　域F上超越元的和未必是F上超越元.

3)　$\alpha=\beta^2$是F上超越元. 事实上，假设$\alpha=\beta^2$是F上代数元，则$\exists F$上非零多项式$f(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_nx^n$，使得$f(\beta^2)=a_0+a_1\beta^2+\cdots+a_{n-1}\beta^{2n-2}+a_n\beta^{2n}=0$，即$\beta$是$F$上非零多项式$g(x)=f(x^2)=a_0+a_1x^2+\cdots+a_{n-1}x^{2(n-1)}+a_nx^{2n}$的根，此与$\beta$是$F$上超越元矛盾.

注　①　该命题说明：

$$\beta\text{是域}F\text{上超越元}\Rightarrow\beta^2\text{是域}F\text{上超越元}.$$

其逆否命题是：

$$\beta^2\text{是域}F\text{上代数元}\Rightarrow\beta\text{是域}F\text{上代数元}.$$

再结合第十六章，一，11，有：

$$\beta^2\text{是域}F\text{上代数元}\Leftrightarrow\beta\text{是域}F\text{上代数元}.$$

其逆否命题是：

$$\beta^2\text{是域}F\text{上超越元}\Leftrightarrow\beta\text{是域}F\text{上超越元}.$$

例　π是$\mathbf{Q}$上超越元$\Rightarrow\pi^2$是$\mathbf{Q}$上超越元.

$\alpha^2=\pi$是$\mathbf{Q}$上超越元$\Rightarrow\alpha$是$\mathbf{Q}$上超越元.

$\alpha^2=\pi$是$\mathbf{R}$上代数元$\Rightarrow\alpha$是$\mathbf{R}$上代数元.

$\alpha^2=\pi$是$\mathbf{Q}(\pi)$上代数元$\Rightarrow\alpha$是$\mathbf{Q}(\pi)$上代数元.

$\alpha^2=\pi$是$\mathbf{Q}(\pi^2)$上代数元$\Rightarrow\alpha$是$\mathbf{Q}(\pi^2)$上代数元.

② 可推广为：设 n 是正整数，则

β^n是域 F 上代数元 $\Leftrightarrow \beta$是域 F 上代数元.

4） $\alpha=\mathrm{i}$ 是 $\mathbb{Z}_7$ 上代数元. i 在 $\mathbb{Z}_7$ 上极小多项式是 x^2+1. $(\mathbb{Z}_7(\mathrm{i}):\mathbb{Z}_7)=2$. $\mathbb{Z}_7(\mathrm{i})\cong\mathbb{Z}_7[x]/(x^2+1)$. $\mathbb{Z}_7(\mathrm{i})=\{a+b\mathrm{i}\mid a,b\in\mathbb{Z}_7\}$.

5） $\alpha=a+b\mathrm{i}$ 在 $\mathbb{Q}$ 上极小多项式是 $[x-(a+b\mathrm{i})][x-(a-b\mathrm{i})]=(x-a)^2+b^2=x^2-2ax+(a^2+b^2)$，从而 α 是 $\mathbb{Q}$ 上代数元. $(\mathbb{Q}(a+b\mathrm{i}):\mathbb{Q})=2$. $\mathbb{Q}(a+b\mathrm{i})\cong\mathbb{Q}[x]/(x^2-2ax+a^2+b^2)$. 因 $a+b\mathrm{i}\in\mathbb{Q}(\mathrm{i})$，$\mathrm{i}=-ab^{-1}+b^{-1}(a+b\mathrm{i})\in\mathbb{Q}(a+b\mathrm{i})$，故 $\mathbb{Q}(a+b\mathrm{i})=\mathbb{Q}(\mathrm{i})=\{c+d\mathrm{i}\mid c,d\in\mathbb{Q}\}$.

例 $3+\mathrm{i}$ 在 $\mathbb{Q}$ 上极小多项式是 $x^2-2\cdot 3x+(3^2+1^2)=x^2-6x+10$.

6） $\alpha=a+b\mathrm{i}$ 是 $\mathbb{R}$ 上代数元. α 在 $\mathbb{R}$ 上极小多项式是 $x^2-2ax+(a^2+b^2)$. 余者与本题5)类似. 最后 $\mathbb{R}(a+b\mathrm{i})=\mathbb{R}(\mathrm{i})=\{c+d\mathrm{i}\mid c,d\in\mathbb{R}\}=\mathbb{C}$. 因此 $\mathbb{C}$ 是 $\mathbb{R}$ 的单代数扩域，从而 $\mathbb{C}$ 是 $\mathbb{R}$ 的代数扩域.

例 $\alpha=-\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}$ 在 $\mathbb{R}$ 上极小多项式是 $x^2-2\left(-\frac{1}{2}\right)x+\left(-\frac{1}{2}\right)^2+\left(\frac{\sqrt{3}}{2}\right)^2=x^2+x+1$.

x^2+x+1 在 $\mathbb{R}$ 上不可约，但在 $\mathbb{R}(\alpha)$ 上，因 α 是 x^2+x+1 的根，即 $x-\alpha\mid x^2+x+1$，而 x^2+x+1除以 $x-\alpha$ 所得商式为 $x+\alpha+1$，故 $x^2+x+1=(x-\alpha)(x+\alpha+1)$.

7） $\alpha=\cos\frac{2\pi}{p}+\mathrm{i}\sin\frac{2\pi}{p}$是 $\mathbb{Q}$ 上代数元. 这是因为 α 是 $\mathbb{Q}$ 上非零多项式 x^p-1 的一个根. 又$x^p-1=(x-1)(x^{p-1}+x^{p-2}+\cdots+1)$，$\alpha$不是$x-1$的根，从而$\alpha$是$x^{p-1}+x^{p-2}+\cdots+1$的根. 由第十五章，四，14，$x^{p-1}+x^{p-2}+\cdots+1$ 在$\mathbb{Q}$上不可约. 于是 α 在$\mathbb{Q}$上极小多项式是 $x^{p-1}+x^{p-2}+\cdots+1$. $(\mathbb{Q}(\alpha):\mathbb{Q})=p-1$. $\mathbb{Q}(\alpha)\cong\mathbb{Q}[x]/(x^{p-1}+x^{p-2}+\cdots+1)$. $\mathbb{Q}(\alpha)=\{a_0+a_1\alpha+\cdots+a_{p-2}\alpha^{p-2}\mid a_i\in\mathbb{Q}\}$.

例 $\alpha=\cos\frac{2\pi}{5}+\mathrm{i}\sin\frac{2\pi}{5}$在 $\mathbb{Q}$ 上极小多项式是 $x^4+x^3+x^2+x+1$. 但 $\alpha=\cos\frac{2\pi}{5}+\mathrm{i}\sin\frac{2\pi}{5}$在 $\mathbb{R}$ 上极小多项式是 $x^2-2\cos\frac{2\pi}{5}x+1$.

8） 因 $\alpha=\cos\frac{2\pi}{12}+\mathrm{i}\sin\frac{2\pi}{12}$(注意，12 不是素数)是$\mathbb{Q}$上非零多项式 $x^{12}-1$ 的一个根，故 α 是$\mathbb{Q}$上代数元. 又 $x^{12}-1=(x^6)^2-1=(x^6-1)(x^2+1)(x^4-x^2+1)$. 因 α 不是 x^6-1 与 x^2+1 的根，故 α 是 x^4-x^2-1 的根. 因 $x^4-x^2+1=(x-\alpha)(x-\alpha^5)(x-\alpha^7)(x-\alpha^{11})$，而 α，α^5，α^7，$\alpha^{11}\overline{\in}\mathbb{Q}$，故 x^4-x^2+1 在$\mathbb{Q}$上无一次因子，也就无三次因子. 在 $x-\alpha$，$x-\alpha^5$，$x-\alpha^7$，$x-\alpha^{11}$中的任两个一次因子的乘积都$\overline{\in}\mathbb{Q}[x]$，于是 x^4-x^2+1 在$\mathbb{Q}$上无二次因子. 所以 x^4-x^2+1在$\mathbb{Q}$上不可约，从而 x^4-x^2+1 是 α 在$\mathbb{Q}$上极小多项式. $(\mathbb{Q}(\alpha):\mathbb{Q})=4$. $\mathbb{Q}(\alpha)\cong\mathbb{Q}[x]/(x^4-x^2+1)$. $\mathbb{Q}(\alpha)=\{a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3\mid a_i\in\mathbb{Q}\}$.

9） $\alpha=\sqrt[3]{2}\varepsilon$ 是$\mathbb{Q}$上代数元. 因 α 是$\mathbb{Q}$上非零多项式 x^3+2 的一个根. 由第十五章，四，13，艾森斯坦因不可约性判别准则，x^3+2 在$\mathbb{Q}$上不可约，从而 x^3+2 是 α 在$\mathbb{Q}$上极小多项

式. $(\mathbf{Q}(\alpha):\mathbf{Q})=3$. $\mathbf{Q}(\alpha)\cong\mathbf{Q}[x]/(x^3+2)$. $\mathbf{Q}(\alpha)=\left\{a_0+a_1\alpha+a_2\alpha^2 \,\middle|\, a_i\in\mathbf{Q}\right\}$.

10) 因 $\alpha=\sqrt[n]{p}$ 是 $\mathbf{Q}$ 上非零多项式 x^n-p 的一个根,故 α 是 $\mathbf{Q}$ 上代数元. 由艾森斯坦因不可约性判别准则,x^n-p 在 $\mathbf{Q}$ 上不可约,从而 x^n-p 是 α 在 $\mathbf{Q}$ 上极小多项式. $(\mathbf{Q}(\alpha):\mathbf{Q})=n$. $\mathbf{Q}(\alpha)\cong\mathbf{Q}[x]/(x^n-p)$. $\mathbf{Q}(\alpha)=\left\{\sum_{i=0}^{n-1}a_i\alpha^i \,\middle|\, a_i\in\mathbf{Q}\right\}$.

例 $\sqrt{5},\sqrt[3]{3},\sqrt[4]{2},\sqrt[5]{7}$ 在 $\mathbf{Q}$ 上极小多项式分别是 x^2-5,x^3-3,x^4-2,x^5-7.

11) $\alpha=1+\sqrt{2}$ 是 $\mathbf{Q}$ 上代数元. α 在 $\mathbf{Q}$ 上极小多项式是 $[x-(1+\sqrt{2})][x-(1-\sqrt{2})]=(x-1)^2-2=x^2-2x-1$. $(\mathbf{Q}(\alpha):\mathbf{Q})=2$. $\mathbf{Q}(\alpha)\cong\mathbf{Q}[x]/(x^2-2x-1)$. $\mathbf{Q}(\alpha)=\left\{a_0+a_1\alpha \,\middle|\, a_i\in\mathbf{Q}\right\}$.

12) $\alpha=\sqrt{1+\sqrt{3}}$ 在 $\mathbf{Q}$ 上是代数元. α 在 $\mathbf{Q}$ 上极小多项式是 $\left(x-\sqrt{1+\sqrt{3}}\right)\left(x+\sqrt{1+\sqrt{3}}\right)\left(x-\sqrt{1-\sqrt{3}}\right)\left(x+\sqrt{1-\sqrt{3}}\right)=[x^2-(1+\sqrt{3})][x^2-(1-\sqrt{3})]=(x^2-1)^2-3=x^4-2x^2-2$.

$(\mathbf{Q}(\alpha):\mathbf{Q})=4$, $\mathbf{Q}(\alpha)\cong\mathbf{Q}[x]/(x^4-2x^2-2)$. $\mathbf{Q}(\alpha)=\left\{a_0+a_1\alpha+a_2\alpha+a_3\alpha^3 \,\middle|\, a_i\in\mathbf{Q}\right\}$.

3. 设下面各 α 在 $\mathbf{Q}$ 上极小多项式为 $p(x)$, $f(\alpha),g(\alpha)\in\mathbf{Q}(\alpha)$. 将 $f(\alpha)+g(\alpha)$ 与 $f(\alpha)g(\alpha)$ 表成最简形式:

1) $p(x)=x^2-2$. $f(\alpha)=3\alpha+4$, $g(\alpha)=5\alpha-6$.

2) $p(x)=x^3-x^2+x+2$, $f(\alpha)=\alpha^2+\alpha+1$, $g(\alpha)=\alpha^2-\alpha$.

解 1) $f(\alpha)+g(\alpha)=8\alpha-2$. $f(x)g(x)=15x^2+2x-24=(x^2-2)15+2x+6$,从而 $f(\alpha)g(\alpha)=2\alpha+6$.

2) $f(\alpha)+g(\alpha)=2\alpha^2+1$. 因 $f(x)g(x)=x^4-x=p(x)(x+1)+(-4x-2)$,又 $p(\alpha)=0$,故 $f(\alpha)g(\alpha)=\alpha^4-\alpha=-4\alpha-2$.

4. 设下面各 α 在域 F 上极小多项式为 $p(x)$, $f(\alpha)(\neq0)\in F(\alpha)$. 求出 $[f(\alpha)]^{-1}$.

1) $\alpha=\sqrt[3]{2}$, $F=\mathbf{Q}$, $p(x)=x^3-2$, $f(\alpha)=\sqrt[3]{4}+\sqrt[3]{2}+1$.

2) $F=\mathbf{Q}$, $p(x)=x^2-x+1$, $f(\alpha)=3\alpha^3-2\alpha^2+\alpha+2$.

3) $F=\mathbf{Z}_3$,把 $\mathbf{Z}_3$ 中元 $[a]$ 表为 a. $p(x)=x^3+2x+1$, $f(\alpha)=\alpha^2$.

4) $p(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+x^n$, $f(\alpha)=\alpha$.

解 求 $[f(\alpha)]^{-1}$ 一般有两种方法.

(i) 因 $p(x)$ 在 F 上不可约,故 $p(x)\mid f(x)$ 或 $p(x),f(x)$ 互素(第十四章,四,6,3)). 因 $f(\alpha)\neq0$,故 $p(x)\nmid f(x)$,否则,若 $p(x)\mid f(x)$,则 $\exists\, q(x)\in F[x]$,使得 $f(x)=p(x)q(x)$,于是 $f(\alpha)=p(\alpha)q(\alpha)=0$,矛盾. 所以 $p(x),f(x)$ 互素. 用辗转相除法可求出 $u(x),v(x)\in F[x]$,使得 $p(x)u(x)+f(x)v(x)=1$. 从而 $p(\alpha)u(\alpha)+f(\alpha)v(\alpha)=1$. 因 $p(\alpha)=0$,故 $f(\alpha)v(\alpha)=1$. 所以 $[f(\alpha)]^{-1}=v(\alpha)$.

(ii) 因 $F(\alpha)$ 中元 $\sum_{i=0}^{n-1}a_i\alpha^i$(其中 $n=\deg p(x)$)的表法唯一,故可直接比较系数.

1) 对 $f(x)=x^2+x+1$, $p(x)=x^3-2$ 作辗转相除法,得 $p(x)(-1)+f(x)(x-1)=1$. 所以 $[f(\alpha)]^{-1}=\alpha-1=\sqrt[3]{2}-1$.

另一解法,设$[f(\alpha)]^{-1}=a+b\alpha+c\alpha^2$,则由$\alpha^3=2$,

$$1=(1+\alpha+\alpha^2)(a+b\alpha+c\alpha^2)$$
$$=a+2b+2c+(a+b+2c)\alpha+(a+b+c)\alpha^2.$$

比较系数,得$a+2b+2c=1$,$a+b+2c=0$,$a+b+c=0$,解得$a=-1$,$b=1$,$c=0$.所以$[f(\alpha)]^{-1}=-1+\alpha=-1+\sqrt[3]{2}$.

注 可将$\dfrac{1+\sqrt[3]{2}}{1+\sqrt[3]{2}+\sqrt[3]{4}}$表成最简形式.

$$\frac{1+\sqrt[3]{2}}{1+\sqrt[3]{2}+\sqrt[3]{4}}=(1+\sqrt[3]{2})(1+\sqrt[3]{2}+\sqrt[3]{4})^{-1}$$
$$=(1+\sqrt[3]{2})(-1+\sqrt[3]{2})=-1+\sqrt[3]{4}.$$

2) 利用辗转相除法,得

$$p(x)(-3x^2-x+1)+f(x)x=1.$$

所以$[f(\alpha)]^{-1}=\alpha$.

注 将$g(\alpha)=\dfrac{\alpha^2+\alpha+1}{3\alpha^3-2\alpha^2+\alpha+2}$表成最简形式.

$$g(\alpha)=(\alpha^2+\alpha+1)(3\alpha^3-2\alpha^2+\alpha+2)^{-1}=(\alpha^2+\alpha+1)\alpha=\alpha^3+\alpha^2+\alpha.$$

用$p(x)$除$g(x)$,得

$$g(x)=x^3+x^2+x=(x^2-x+1)(x+2)+2x-2.$$

所以$g(\alpha)=2\alpha-2$.

3) 设$[f(\alpha)]^{-1}=a\alpha^2+b\alpha+c$.因$\alpha^3=-2\alpha-1$,故$\alpha^2(a\alpha^2+b\alpha+c)=a\alpha^4+b\alpha^3+c\alpha^2=(-2a+c)\alpha^2+(-a-2b)d-b=1$.比较系数,得$-2a+c=0$,$-a-2b=0$,$-b=1$,解得$a=2$,$b=2$,$c=1$.所以$[f(\alpha)]^{-1}=2\alpha^2+2\alpha+1$.

4) 设$[f(\alpha)]^{-1}=\alpha^{-1}=b_0+b_1\alpha+\cdots+b_{n-2}\alpha^{n-2}+b_{n-1}\alpha^{n-1}$.因$f(\alpha)[f(\alpha)]^{-1}=1$,故$b_0\alpha+b_1\alpha^2+\cdots+b_{n-2}\alpha^{n-1}+b_{n-1}\alpha^n=1$.用$\alpha^n=-a_0-a_1\alpha-a_2\alpha^2-\cdots-a_{n-1}\alpha^{n-1}$代入,整理,比较系数,得$-a_0b_{n-1}=1$,$b_0-b_{n-1}a_1=0$,$b_1-b_{n-1}a_2=0$,$\cdots$,$b_{n-2}-b_{n-1}a_{n-1}=0$.其中$a_0\neq 0$.事实上,若$a_0=0$,当$n=1$时,$p(x)=x$只能是0在$F$上极小多项式,从而$f(\alpha)=\alpha=0$,矛盾;当$n>1$时,$p(x)=x(a_1+a_2x+\cdots+a_{n-1}x^{n-2}+x^{n-1})$,此与$p(x)$在$F$上不可约矛盾.所以$a_0\neq 0$.$\exists a_0^{-1}\in F$.于是$b_{n-1}=-a_0^{-1}$,$b_0=-a_1a_0^{-1}$,$b_1=-a_2a_0^{-1}$,$\cdots$,$b_{n-2}=-a_{n-1}a_0^{-1}$.从而$[f(\alpha)]^{-1}=\alpha^{-1}=-a_1a_0^{-1}-a_2a_0^{-1}\alpha-\cdots-a_{n-1}a_0^{-1}\alpha^{n-2}-a_0^{-1}\alpha^{n-1}$.

5. 求出下面各域E在域F上的次数和一个基.

1) $E=\mathbf{Q}(\sqrt{2},\sqrt[3]{3})$, $F=\mathbf{Q}$.

2) $E=\mathbf{Q}(\sqrt[4]{2},\mathrm{i})$, $F=\mathbf{Q}$.

3) $E=\mathbf{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$, $F=\mathbf{Q}$.

解 1) 因$\sqrt[3]{3}$在$\mathbf{Q}(\sqrt{2})$上极小多项式是x^3-3,$\sqrt{2}$在$\mathbf{Q}$上极小多项式是x^2-2,故

$$(\mathbf{Q}(\sqrt{2},\sqrt[3]{3}):\mathbf{Q})=(\mathbf{Q}(\sqrt{2})(\sqrt[3]{3}):\mathbf{Q}(\sqrt{2}))(\mathbf{Q}(\sqrt{2}):\mathbf{Q})=3\times 2=6.$$

因$1,\sqrt[3]{3},\sqrt[3]{9}$是$\mathbf{Q}(\sqrt{2})(\sqrt[3]{3})$在$\mathbf{Q}(\sqrt{2})$上的一个基,$1,\sqrt{2}$是$\mathbf{Q}(\sqrt{2})$在$\mathbf{Q}$上的一个基,故由第十六章,一,9中定理的证明知,$1,\sqrt{2},\sqrt[3]{3},\sqrt[3]{9},\sqrt{2}\sqrt[3]{3},\sqrt{2}\sqrt[3]{9}$是$\mathbf{Q}(\sqrt{2},\sqrt[3]{3})$在$\mathbf{Q}$上的一个基.

2)　因 i 在 $\mathbf{Q}(\sqrt[4]{2})$ 上极小多项式是 x^2+1，$\sqrt[4]{2}$ 在 $\mathbf{Q}$ 上极小多项式是 x^4-2，故

$$(\mathbf{Q}(\sqrt[4]{2},\mathrm{i}):\mathbf{Q})=(\mathbf{Q}(\sqrt[4]{2})(\mathrm{i}):\mathbf{Q}(\sqrt[4]{2}))(\mathbf{Q}(\sqrt[4]{2}):\mathbf{Q})=2\times4=8.$$

因 1，i 是 $\mathbf{Q}(\sqrt[4]{2})(\mathrm{i})$ 在 $\mathbf{Q}(\sqrt[4]{2})$ 上的一个基，$1,\sqrt[4]{2},\sqrt[4]{4},\sqrt[4]{8}$ 是 $\mathbf{Q}(\sqrt[4]{2})$ 在 $\mathbf{Q}$ 上的一个基，故 $1,\sqrt[4]{2},\sqrt[4]{4},\sqrt[4]{8},\mathrm{i},\mathrm{i}\sqrt[4]{2},\mathrm{i}\sqrt[4]{4},\mathrm{i}\sqrt[4]{8}$ 是 $\mathbf{Q}(\sqrt[4]{2},\mathrm{i})$ 在 $\mathbf{Q}$ 上的一个基.

3)　$(\mathbf{Q}(\sqrt{2},\sqrt{3},\sqrt{5}:\mathbf{Q})=(\mathbf{Q}(\sqrt{2},\sqrt{3})(\sqrt{5}):\mathbf{Q}(\sqrt{2},\sqrt{3}))(\mathbf{Q}(\sqrt{2})(\sqrt{3}):\mathbf{Q}(\sqrt{2}))\cdot(\mathbf{Q}(\sqrt{2}):\mathbf{Q})=2\cdot2\cdot2=8$. $1,\sqrt{2},\sqrt{3},\sqrt{6},\sqrt{5},\sqrt{10},\sqrt{15},\sqrt{30}$ 是 $\mathbf{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ 在 $\mathbf{Q}$ 上的一个基.

四、思考问题

1. 证明：

1)　域 E 的任一子域 F 都包含 E 的素子域 Δ.

2)　$\mathbf{Q}(\sqrt{\pi},\sqrt[4]{\pi},\pi,\pi^{100})=\mathbf{Q}(\sqrt[4]{\pi})$.

3)　设 α 在域 F 上的次数为 n，则

$$a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}=0,\ a_i\in F\Leftrightarrow a_0=a_1=\cdots a_{n-1}=0.$$

4)　设 E 是域 F 的代数扩域，$f(x),g(x)$ 在 $F[x]$ 中互素，则 $f(x),g(x)$ 也在 $E[x]$ 中互素.

5)　若 $p(x)$ 是域 F 上 3 次不可约多项式，E 是 F 的有限扩域且 $(E:F)=2^m$，则 $p(x)$ 在 E 上也不可约.

6)　设 K 是 $\mathbf{Q}$ 的扩域，$\mathbf{Q}\subset K\subset\mathbf{Q}(\sqrt[7]{2})$，则 $K=\mathbf{Q}(\sqrt[7]{2})$ 或 $K=\mathbf{Q}$.

2. 设 E 是域 F 的有限扩域，$p(x)$ 是 F 上的最高系数为 1 的次数大于 1 的不可约多项式，且 $\deg p(x)$ 与 $(E:F)$ 互素. 证明：$p(x)$ 在 E 中没有根.

3. 设 E 是域 F 的有限扩域，且对于包含 F 的任意两个 E 的子域 I_1 和 I_2，$I_1\subset I_2$ 或 $I_2\supset I_1$. 证明：E 是 F 的单扩域.

4. 设 α 是域 F 上超越元，$E=F(\alpha)$. 又设 $I=F\left(\dfrac{\alpha^3}{\alpha+1}\right)$. 证明：$E$ 是 I 的单代数扩域.

5. 设 α 是域 F 上超越元，$E=F(\alpha)$，$I(\supsetneqq F)$ 是 E 的子域. 证明：α 是 I 上代数元.

6. 设 E 是域 F 的扩域. 证明：存在 F 的代数扩域 K，且 $\forall\alpha\in E$，$\alpha\overline{\in}K$，α 都是 K 上超越元.

7. 设域 F 的特征是素数 p，n 是正整数，$d^{p^n}=\beta\in F$ 而 $\alpha^{p^{n-1}}\overline{\in}F$. 证明：$x^{p^n}-\beta$ 是 F 上不可约多项式.

8. 证明：设 E 是域 F 的代数扩域，则 E 的任一包含 F 的子环 R 都是 E 的子域. 若 E 是域 F 的有限扩域，结论也成立.

9. 设 E 是 $\mathbf{R}$ 的有限扩域，证明：$E\cong\mathbf{R}$ 或 $E\cong\mathbf{C}$.

10. 设 F 是域，$E=F(\alpha)$，α 是 F 上奇次代数元. 证明：$E=F(\alpha^2)$.

第十七章　多项式的分裂域、有限域、可离扩域

一、基本问题问答

1. 给出代数闭域的定义及一些等价形式.

答　设 E 是域.

E 是代数闭域 $\Leftrightarrow$ E 无真代数扩域

$\Leftrightarrow \forall f(x)\in E[x]$, $\deg f(x)>0$, 则 $f(x)$ 在 E 中都有一个根

$\Leftrightarrow \forall f(x)\in E[x]$, $\deg f(x)>0$, 则 $f(x)$ 的全部根都 $\in E$

$\Leftrightarrow \forall f(x)\in E[x]$, $\deg f(x)>0$, 则 $f(x)$ 在 E 上可分解为一次因子的乘积.

例　复数域 $\mathbb{C}$ 是代数闭域.

2. 1)　证明命题:设 E 是域 F 的扩域,给定 $f(x)\in F[x]$, $\deg f(x)=n>0$, $f(x)=a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, $a_n\in F$, $\alpha_i\in E$. 若 E 是 $f(x)$ 在 F 上的分裂域,则 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$①.

2)　证明该命题的逆命题:设 E 是域 F 的扩域,给定 $f(x)\in F[x]$, $\deg f(x)=n>0$, $f(x)=a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, $a_n\in F$, $\alpha_i\in E$. 若 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$, 则 E 是 $f(x)$ 在 F 上的分裂域.

证　1)　由已知, $F\subset F(\alpha_1,\alpha_2,\cdots,\alpha_n)\subset E$, $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是 E 的子域. 因 $\alpha_i\in F(\alpha_1,\alpha_2,\cdots,\alpha_n)$, 故 $f(x)$ 在 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 上可分解为一次因子的乘积. 又 E 是 $f(x)$ 在 F 上的分裂域,从而 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 不是 E 的真子域. 所以 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)=E$.

2)　因 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是含 F 与 $f(x)$ 的所有根的最小域,故 E 的任一真子域 I: $F\subset I\subsetneqq E$, 不可能含 $f(x)$ 的所有根. 从而 $f(x)$ 在 I 上不能分解为一次因子的乘积. 所以 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是 $f(x)$ 在 F 上的分裂域.

注　1)　设 F 是域, $f(x)\in F[x]$, $\deg f(x)=n\geqslant 1$, 则 E 是 $f(x)$ 在 F 上的分裂域 $\Leftrightarrow$

(i)　$f(x)=a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, $a_n\in F$, $\alpha_i\in E$.

(ii)　$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$.

"分裂"的含义是指 $f(x)$ 能在域 E 上分解为一次因子的乘积. 但 E 仅满足此条件, E 未必是 $f(x)$ 在 F 上的分裂域,还得满足最小性,即 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$. 例, $x^3-5(\in\mathbb{Q}[x])$ 在 $\mathbb{C}$ 上能分解为一次因子的乘积: $x^3-5=(x-\sqrt[3]{5})(x^2+\sqrt[3]{5}x+\sqrt[3]{25})=(x-\sqrt[3]{5})(x-\omega\sqrt[3]{5})(x-\omega^2\sqrt[3]{5})$, 其中 $\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}$, $\omega^2=-\frac{1}{2}-\frac{\sqrt{3}}{2}\mathrm{i}$. 但 $\mathbb{C}$ 不是 x^3-5 在 $\mathbb{Q}$ 上的分裂域 $\mathbb{Q}(\sqrt[3]{5},\omega\sqrt[3]{5},$

---

①　张禾瑞. 近世代数基础. 北京:高等教育出版社,1978. 165. 定理 1.

$\omega^2\sqrt[3]{5}) = \mathbf{Q}(\sqrt[3]{5},\omega) = \mathbf{Q}(\sqrt[3]{5},\sqrt{3}\,\mathrm{i})$.

当然仅有 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$，$E$ 未必是 $f(x)$ 在 F 上的分裂域. 例，$E=\mathbf{Q}(\sqrt[3]{2})$ 不是 x^3-2 在 $\mathbf{Q}$ 上的分裂域 $\mathbf{Q}(\sqrt[3]{2},\omega\sqrt[3]{2},\omega^2\sqrt[3]{2})=\mathbf{Q}(\sqrt[3]{2},\omega)$，其中 $\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}$.

2) $f(x)$ 在域 F 上的分裂域 E 是含 F 和 $f(x)$ 的所有根 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 的 F 的最小扩域，即 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$. 于是 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是 F 的有限扩域，从而 E 是 F 的代数扩域.

3) $f(x)$ 的分裂域与域 F 有关.

例 $x^4-2\in\mathbf{Q}[x]\subset\mathbf{R}[x]$. $x^4-2=(x-\sqrt[4]{2})(x+\sqrt[4]{2})(x-\mathrm{i}\sqrt[4]{2})(x+\mathrm{i}\sqrt[4]{2})$. x^4-2 在 $\mathbf{Q}$ 上的分裂域是 $\mathbf{Q}(\sqrt[4]{2},-\sqrt[4]{2},\mathrm{i}\sqrt[4]{2},-\mathrm{i}\sqrt[4]{2})=\mathbf{Q}(\sqrt[4]{2},\mathrm{i}\sqrt[4]{2})=\mathbf{Q}(\sqrt[4]{2},\mathrm{i})$. 而 x^4-2 在 $\mathbf{R}$ 上的分裂域是 $\mathbf{R}(\sqrt[4]{2},\mathrm{i})=\mathbf{R}(\mathrm{i})=\mathbf{C}$.

3. 证明命题：设 F 是域，$f(x)\in F[x]$，$\deg f(x)=n>0$，则 $f(x)$ 在 F 上的分裂域 E 必存在[①].

证 因 $\deg f(x)=n>0$，故 $f(x)\neq 0$，$f(x)\neq$ 单位. 又 $F[x]$ 是唯一分解环，从而 $\exists$ 最高系数为 1 的不可约多项式 $f_1(x)\in F[x]$，使得 $f(x)=f_1(x)g_1(x)$，其中 $g_1(x)\in F[x]$. 由第十六章，二，4，$\exists F$ 的单代数扩域 $E_1=F(\alpha_1)$，且 $f_1(\alpha_1)=0$. 在 $E_1[x]$ 里，由 $f_1(\alpha_1)=0$，$f(\alpha_1)=0$，从而 $x-\alpha_1 \mid f(x)$，即 $f(x)=(x-\alpha_1)h_1(x)$，其中 $h_1(x)\in E_1[x]$，$h_1(x)\neq 0$，$\deg h_1(x)<\deg f(x)$. 若 $h_1(x)=$ 单位，则 $E_1=F(\alpha_1)$ 是 $f(x)$ 在 F 上的分裂域. 若 $h_1(x)\neq$ 单位. 因 $E_1[x]$ 是唯一分解环，故 $\exists$ 最高系数为 1 的不可约多项式 $f_2(x)\in E_1[x]$，使得 $h_1(x)=f_2(x)g_2(x)$，即 $f(x)=(x-\alpha_1)f_2(x)g_2(x)$，其中 $g_2(x)\in E_1[x]$. 由第十六章，二，4，$\exists E_1$ 的单代数扩域 $E_2=E_1(\alpha_2)=F(\alpha_1,\alpha_2)$，且 $f_2(\alpha_2)=0$. 在 $E_2[x]$ 里，由 $f_2(\alpha_2)=0$，$h_1(\alpha_2)=0$，从而 $x-\alpha_2 \mid h_1(x)$，即 $h_1(x)=(x-\alpha_2)h_2(x)$. 于是 $f(x)=(x-\alpha_1)(x-\alpha_2)h_2(x)$，其中 $h_2(x)\in E_2[x]$，$h_2(x)\neq 0$，$\deg h_2(x)<\deg h_1(x)$. 若 $h_2(x)=$ 单位，则 $E_2=F(\alpha_1,\alpha_2)$ 是 $f(x)$ 在 F 上的分裂域. 若 $h_2(x)\neq$ 单位，则仿上继续做下去. 因 $\deg f(x)=n$ 是一个有限正整数，故经有限步骤后，有

$$f(x)=a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),$$

$\alpha_i\in E$，$a_n\in F$，则 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是 $f(x)$ 在 F 上的一个分裂域.

注 该定理称为分裂域的存在定理. 解决了域 F 上任一多项式 $f(x)(\overline{\in} F)$，存在 F 的适当扩域 E，使 $f(x)$ 的全部根都 $\in E$. 还可用数学归纳法证明. 证明中主要利用单代数扩域的存在定理.

4. 证明命题：设域 $L\overset{\eta}{\cong}\overline{L}$，$L[x]\overset{\lambda}{\cong}\overline{L}[x]$，且 λ 保持 η，即 $\forall a\in L\subset L[x]$，有 $\lambda(a)=\overline{a}=\eta(a)$. 又设 $p(x)$ 在域 L 上不可约. 证明：$p(x)$ 在 λ 下的象 $\overline{p}(x)$ 在域 $\overline{L}$ 上也不可约[②].

证 假设 $\overline{p}(x)$ 在 $\overline{L}$ 上不是不可约. 因 $p(x)\neq 0$，$\neq$ 单位，故 $\overline{p}(x)\neq 0$，$\neq$ 单位，从而 $\overline{p}(x)$ 在 $\overline{L}$ 上可约，$\overline{p}(x)$ 在 $\overline{L}$ 上有真因子 $\overline{g}(x)$，使得 $\overline{p}(x)=\overline{g}(x)\overline{h}(x)$，其中 $\overline{h}(x)$ 也是 $\overline{p}(x)$

---

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 166. 定理 2.

② 同上. 167. 引理 2.

在 $\bar{L}$ 上的真因子.从而在 λ 下,$p(x)=g(x)h(x)$,其中 $g(x)\neq$ 单位[①].否则 $\bar{g}(x)=$ 单位,与 $\bar{g}(x)$ 是 $\bar{p}(x)$ 的真因子矛盾.同理 $h(x)\neq$ 单位.由第十四章,一,6,$p(x)$ 有真因子,此与 $p(x)$ 在 L 上不可约矛盾.所以 $\bar{p}(x)$ 在 $\bar{L}$ 上不可约.

注 该命题是第十六章,一,7 的推广,只要取 $\bar{L}=L$ 即可.且其证明类似.

5. 1) 证明命题:设 E 是 $f(x)$ 在域 F 上的分裂域,则 $\forall\beta\in E$,β 在 F 上极小多项式 $g(x)$ 在 E 上能分解为一次因子的积[②].

2) 证明该命题的逆命题:设 E 是域 F 的有限扩域,$\forall\beta\in E$,β 在 F 上极小多项式在 E 上能分解为一次因子的积,则 E 是 F 上某个多项式 $f(x)$ 在 F 上的分裂域.

证 1) 因 E 是 $f(x)$ 在 F 上的分裂域,故 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$,其中 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 $f(x)$ 的全部根.因 E 是 F 的代数扩域,故 $\forall\beta\in E$,β 是 F 上代数元,从而 β 在 F 上极小多项式 $g(x)$ 必存在.假设 $g(x)$ 在 E 上不能分解为一次因子的积,则 $\deg g(x)>1$.在 $E[x]$ 里,$g(\beta)=0$,即 $x-\beta\mid g(x)$,于是 $g(x)=(x-\beta)h(x)$,其中 $h(x)\in E[x]$,$h(x)\neq0$.因 $\deg g(x)>1$,故 $h(x)\neq$ 单位.因 $E[x]$ 是唯一分解环,故 $\exists$ 最高系数为 1 的 E 上不可约多项式 $p(x)$,使得 $h(x)=p(x)g_1(x)$,其中 $g_1(x)\in E[x]$,且 $\deg p(x)=m>1$.事实上,假定 $h(x)$ 只有 E 上一次不可约因子,就与 $g(x)=(x-\beta)h(x)$ 在 E 上不能分解为一次因子的积矛盾.于是 $g(x)=(x-\beta)p(x)g_1(x)$.由第十六章,二,4,$\exists E$ 的单代数扩域 $E(\beta')$,$p(x)$ 是 β' 在 E 上极小多项式,所以 $(E(\beta'):E)=\deg p(x)=m$[③].

因 $g(\beta')=(\beta'-\beta)p(\beta')g_1(\beta')=0$,又 $g(x)\in F[x]$,$g(x)$ 在 F 上不可约,故 β' 是 F 上代数元,且 $g(x)$ 是 β' 在 F 上极小多项式.又 β 是 F 上代数元,$g(x)$ 也是 β 在 F 上极小多项式,所以由第十六章,一,7,$F(\beta')\cong F(\beta)$.且 $F(\beta')[x]\cong F(\beta)[x]$,$f(x)\to f(x)$(因 $f(x)\in F[x]$).因此 $f(x)$ 在 $F(\beta')$ 上的分裂域 $\cong f(x)$ 在 $F(\beta)$ 上的分裂域[④],即 $F(\beta')(\alpha_1,\alpha_2,\cdots,\alpha_n)\cong F(\beta)(\alpha_1,\alpha_2,\cdots,\alpha_n)$,即 $F(\alpha_1,\alpha_2,\cdots,\alpha_n,\beta')\overset{\phi}{\cong}F(\alpha_1,\alpha_2,\cdots,\alpha_n,\beta)$.从而 $F(\alpha_1,\alpha_2,\cdots,\alpha_n,\beta')$,$F(\alpha_1,\alpha_2,\cdots,\alpha_n,\beta)$ 都是 E 的有限扩域,即它们都是 E 上有限维空间.而 ϕ 是它们间的一一映射,保持加法.且因 $\forall a\in F$,$\phi(a)=a$,故 $\forall\gamma\in F(\alpha_1,\alpha_2,\cdots,\alpha_n,\beta')$,$\phi(a\gamma)=\phi(a)\phi(\gamma)=a\phi(\gamma)$.因此 ϕ 是这两个向量空间 $F(\alpha_1,\alpha_2,\cdots,\alpha_n,\beta')$ 与 $F(\alpha_1,\alpha_2,\cdots,\alpha_n,\beta)$ 间的同构映射.于是它们的维数相等,即 $(F(\alpha_1,\alpha_2,\cdots,\alpha_n,\beta'):F)=(F(\alpha_1,\alpha_2,\cdots,\alpha_n,\beta):F)$.

$$(F(\alpha_1,\alpha_2,\cdots,\alpha_n,\beta'):F)=(E(\beta'):F)=(E(\beta'):E)(E:F)=m(E:F).$$

$$(F(\alpha_1,\alpha_2,\cdots,\alpha_n,\beta'):F)=(E(\beta):F)=(E:F)(\text{因 }\beta\in E).$$

所以 $m(E:F)=(E:F)$.因 $(E:F)\neq0$,故 $m=1$,此与 $m>1$ 矛盾.从而 $g(x)$ 在 E 上能分解为一次因子的积.

2) 已知 E 是 F 的有限扩域,由第十六章,二,9,$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$.令 α_i 在 F 上极小多项式是 $p_i(x)$,$i=1,2,\cdots,n$,且 $f(x)=p_1(x)p_2(x)\cdots p_n(x)$.由已知条件,$p_i(x)$ 在 E 上能分解为一次因子的积,从而 $f(x)$ 的全部根都在 E 内,于是 E 含 $f(x)$ 在 F 上的分裂域 E':$E\supset E'$;反之,因 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 都是 $f(x)$ 的根,故 $E'\supset F(\alpha_1,\alpha_2,\cdots,\alpha_n)=E$.所以 $f(x)$ 在

---

① 张禾瑞.近世代数基础.北京:高等教育出版社,1978.167.引理 1.

② 同上.170.定理 4.

③ 同上.163.推论 2.

④ 同上.168.定理 3.

F 上的分裂域 $E'=E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$.

注　1)　由该命题知,若 E 是 $f(x)$ 在域 F 上的分裂域,$\forall \beta\in E$,则 β 在 F 上极小多项式在 F 上的分裂域是 E 的子域.

2)　域 F 上任一多项式 $g(x)$ 在 $f(x)$ 的分裂域上未必能分解为一次因子的积.

例　$x^4-5x^2+6=(x^2-2)(x^2-3)=(x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{3})(x+\sqrt{3})$ 在 $\mathbb{Q}$ 上的分裂域是 $E=\mathbb{Q}(\sqrt{2},\sqrt{3})$. 但 $\mathbb{Q}$ 上多项式 x^2-5 在 E 上不能分解为一次因子的积. 而 $\sqrt{2}(\in E)$ 在 $\mathbb{Q}$ 上极小多项式 x^2-2 在 E 上能分解为一次因子的积.

6. 命题:设 E 是有限域,ch $E=$ 素数 p,Δ 是 E 的素子域,E 中恰含 $q=p^n$ 个元,n 是正整数,则

1)　E 是多项式 $x^q-x(\in\Delta[x])$ 在 Δ 上的分裂域.

2)　若 I 是有限域,ch $I=$ 素数 p,Ω 是 I 的素子域,I 中恰含 $q=p^n$ 个元,n 是正整数,于是 $E\cong I$[①].

试证明 2).

证　由第十一章,三,9,1),ch $\Delta=$ ch $\Omega=p$,又 Δ,Ω 都是素域,有 $\Delta\cong\mathbb{Z}/(p)$,$\Omega\cong\mathbb{Z}/(p)$[②],从而 $\Delta\cong\Omega$. 且 $\Delta[x]\cong\Omega[x]$. 所以 x^q-x 在 Δ 上的分裂域 E 与 x^q-x 在 Ω 上的分裂域 I 同构.

注　元的个数相同的群未必同构(见第七章,二,11). 元的个数相同的环也未必同构(由第九章,二,2,$R=\{0,a,b,c\}$ 为非交换环,而 $\mathbb{Z}_4$ 为交换环,它们不同构). 但我们有下面命题:设 E_1,E_2 是两个有限域,则

$$E_1,E_2\text{ 的元的个数相同}\Leftrightarrow E_1\cong E_2.$$

事实上,($\Rightarrow$)　记 E_1,E_2 所含元的个数为 q. 则 $\exists$ 素数 p_1,p_2,正整数 n_1,n_2,使 $q=p_1^{n_1}=p_2^{n_2}$[③],于是 $p_1\mid p_2^{n_2}$,$p_2\mid p_1^{n_1}$. 因 p_1,p_2 是素数,故 $p_1\mid p_2$,$p_2\mid p_1$. 又 p_1,p_2 都是正整数,从而 $p_1=p_2$,于是 $n_1=n_2$. 于是 E_1,E_2 所含元的个数都是 $q=p_1^{n_1}$. 由该定理知 $E_1\cong E_2$. ($\Leftarrow$) 显然成立.

该命题说明,有限域的代数性质由该域的元的个数唯一确定. 这是因为有限域的结构比其他代数系数更为严谨.

7. 关于命题:任意给定一个素数 p,一个正整数 n. 设 Δ 是特征为 p 的素域,$q=p^n$,E 是 x^q-x 在 Δ 上的分裂域,则 E 是含 q 个元的有限域[④].

1)　为何 $f(x)=x^q-x$ 在 E 中的 q 个根 $\alpha_1,\alpha_2,\cdots,\alpha_q$ 都互不相同?

2)　为何 $E_1=\{\alpha_1,\alpha_2,\cdots,\alpha_q \mid \alpha_1,\alpha_2,\cdots,\alpha_q$ 是 x^q-x 的不同的 q 个根$\}$ 是 $E=\Delta(\alpha_1,\alpha_2,\cdots,\alpha_q)$ 的子域?

3)　为何 $E=E_1$?

答　1)　因 $f'(x)=qx^{q-1}-1=p^n(1x^{q-1})-1=[p^{n-1}(p\cdot 1)]x^{q-1}-1=-1$(因 ch $\Delta=p$),

---

① 张禾瑞. 近世代数基础. 北京:高等教育出版社,1978. 172. 定理 2.

② 同上. 152. 定理 2.

③ 同上. 171. 定理 1.

④ 同上. 173. 定理 3.

故 $x-\alpha_i \nmid f'(x), i=1,2,\cdots,q$. 所以 α_i 不是 x^q-x 的重根[①]，从而 x^q-x 无重根.

2) 显然 $\varnothing \neq E_1 \subset E$. 又因 $q=p^n \geqslant p \geqslant 2$，故 E_1 中至少有一个不等于零的元. $\forall \alpha_i,\alpha_j \in E_1$，由第十一章，三，9，1），$E$ 是特征为 p 的域. 由第十章，三，4，2），

$$(\alpha_i-\alpha_j)^q=(\alpha_i-\alpha_j)^{p^n}=\alpha_i^{p^n}-\alpha_j^{p^n}=\alpha_i-\alpha_j,$$

从而 $\alpha_i-\alpha_j \in E_1$. $\forall \alpha_i,\alpha_j(\neq 0) \in E_1$，

$$(\alpha_i\alpha_j^{-1})^q=\alpha_i^q(\alpha_j^q)^{-1}=\alpha_i\alpha_j^{-1},$$

从而 $\alpha_i\alpha_j^{-1} \in E_1$. 所以 E_1 是 E 的子域.

3) 因 Δ 是 $E=\Delta(\alpha_1,\alpha_2,\cdots,\alpha_q)$ 的素子域，E_1 是 E 的子域，故由第十六章，四，1，1）知 $E_1 \supset \Delta$. 从而 E_1 是含 Δ 与 $\alpha_1,\alpha_2,\cdots,\alpha_q$ 的域. 又 E 是含 Δ 与 $\alpha_1,\alpha_2,\cdots,\alpha_q$ 的最小域，因此 $E \subset E_1$. 反之，显然 $E_1 \subset E$. 所以 $E=E_1$.

注 1) 任给素数 p 及正整数 n，由 $x^{p^n}-x$ 在特征为 p 的素域 Δ 上的分裂域的存在性知含 p^n 个元的有限域必存在.

2) 该命题是第十七章，一，6 的逆定理. 即：设 Δ 是特征为素数 p 的素域，n 是任一正整数，$q=p^n$，则

E 是以 Δ 为素子域的含 q 个元的有限域

$\Leftrightarrow E$ 是多项式 x^q-x 在 Δ 上的分裂域.

3) 设 n 是一个正整数，p 是一个素数，则 E 是含 p^n 个元的有限域，$\mathrm{ch}\,E=p$，$(E:\Delta)=n$，Δ 是 E 的素子域

$\Leftrightarrow E$ 是 $x^{p^n}-x$ 在 Δ 上的分裂域，Δ 是特征为 p 的 E 的素子域，$(E:\Delta)=n$

$\Leftrightarrow E=\{\alpha_1,\alpha_2,\cdots,\alpha_{p^n} \mid \alpha_1,\alpha_2,\cdots,\alpha_{p^n}$ 是 $x^{p^n}-x$ 的全部不同的根$\}$，$p=\mathrm{ch}\,E$，

$n=(E:\Delta)$，Δ 是 E 的素子域.

4) 由于最初是伽罗华(Galois)对有限域作过公理化的研究，因此有限域又称做 Galois 域. 因为对于任一素数 p 和正整数 n，有且只有一个含 p^n 个元的有限域，所以将此有限域记为 $GF(p^n)$.

8. 证明：设 G 是一个有限交换群，m 是 G 的所有元的阶中最大者，则 $\forall a \in G$，a 的阶 $|a| \mid m$[②].

证 因 G 是有限群，故由第四章，二，6，G 的所有元的阶都有限，从而 $\exists m$ 是 G 的所有元的阶中最大者. 假定 $\exists c \in G$，$|c|=n \nmid m$，则 $n \neq 1$. 因整数环 $\mathbb{Z}$ 是唯一分解环，故

$$n=p_1^{j_1},p_2^{j_2}\cdots p_t^{j_t},$$

其中 p_u 是不同素数，$j_u>0$. 令

$$m=p_1^{i_1}\,p_2^{i_2}\cdots p_t^{i_t}\,q_1^{k_1}\,q_2^{k_2}\cdots q_s^{k_s},$$

其中 p_u,q_v 是互不相同的素数，$i_u \geqslant 0$，$k_v>0$. 则必存在素数 p，不妨设 $p=p_1$，记 $i_1=i$，$j_1=j$，使 $j>i$（不然，若每 $j_u \leqslant i_u$，则 $n \mid m$，矛盾）. 于是 $n=p^jn_1$，其中 $n_1=p_2^{j_2}\cdots p_t^{j_t}$，$m=p^im_1$，其中 $m_1=p_2^{i_2}\cdots p_t^{i_t}q_1^{k_1}q_2^{k_2}\cdots q_s^{k_s}$，且 $(p,m_1)=1$. 设以 m 为阶的元为 $d \in G$. 则由第六章，二，5，$|d^{p^i}|=\dfrac{m}{(m,p^i)}=$

---

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 150. 定理 3.

② 同上. 173. 引理.

$\frac{m}{p^i}=m_1$. 因$|c|=n$,故$|c^{n_1}|=\frac{n}{(n,n_1)}=\frac{n}{n_1}=p^j$(见第七章,一,9). 因$(p,m_1)=1$,故$(p^j,m_1)=1$. 又$G$是交换群,从而由第七章,二,8,有$d^{p^i}c^{n_1}\in G$,使

$$|d^{p^i}c^{n_1}|=|d^{p^i}|\cdot|c^{n_1}|=m_1p^j>m_1p^i=m,$$

此与已知条件矛盾. 所以$\forall a\in G,|a|\,\big|\,m$.

注　若G不是交换群,命题不成立. 例,S_3不是交换群,$|(1)|=1$,$|(1\ 2)|=|(2\ 3)|=|(1\ 3)|=2$,$|(1\ 2\ 3)|=|(1\ 3\ 2)|=3$,从而3是$S_3$的所有元的阶中最大者,但$2\nmid 3$.

9.　关于命题:设E是有限域,Δ是E的素子域,则E是Δ的单扩域①. 在证明了含q个元的有限域E的乘群G是一个循环群$G=(\alpha)$以后,为何$E=\Delta(\alpha)$?

答　因$G=(\alpha)=\{1,\alpha,\cdots,\alpha^{q-2}\}$,故$E=\{0,1,\alpha,\cdots,\alpha^{q-2}\}\subset\Delta(\alpha)$;反之,因$E$是含$\Delta$与$\alpha$的域,$\Delta(\alpha)$是含$\Delta$与$\alpha$的最小域,故$\Delta(\alpha)\subset E$. 所以$E=\Delta(\alpha)$.

注　1)　含p^n个元的有限域E的乘群G是一个p^n-1阶循环群,其中$p=\mathrm{ch}\,E$,$n=(E:\Delta)$,Δ是E的素子域. 若α的阶是G的所有元的阶中最大者,则$G=(\alpha)$且$E=\Delta(\alpha)$. 因为单扩域的结构是清楚的,所以有限域的结构也就清楚了. 因此该命题完全揭露了有限域的构造.

2)　可推广为如下命题:任一域E的乘群的有限子群H是循环群.

事实上,因H是有限交换群,设m是H的所有元的阶中最大者,故由第十七章,一,8,$\forall a\in H,|a|\,\big|\,m$,从而$a^m=1$. 设$|H|=n$,则$H$的$n$个元都是$m$次多项式$x^m-1(\in E[x])$的根. 且$n\leqslant m$②. 又因$m$是$H$中某元$b$的阶,故$m\,\big|\,n$. 又$n\neq 0$,因此$m\leqslant n$. 于是$|b|=m=n=|H|$. 所以$H=(b)$.

10. 判断下面各命题是否正确.

1)　设E是域F的扩域,$\alpha\in E$,而α在F上极小多项式在F中有重根,则α不是F上可离元.

2)　设$\alpha\in$域F,则α是F上可离元.

3)　域F的可离扩域必存在.

答　1)　不正确. 首先E得是F的代数扩域,非可离元α是F上代数元,才能谈到α在F上极小多项式. 再者α在F上极小多项式是F上的不可约多项式,在F中不可能有重根. 因此对于极小多项式是否有重根的问题,总是在分裂域中来谈的. 正确的说法是:设E是域F的代数扩域,$\alpha\in E$,则

α不是F上可离元$\Leftrightarrow\alpha$在F上极小多项式在分裂域中有重根.

2)　正确. 事实上,设$p(x)$是α在F上极小多项式. 因$\alpha\in F$,故由第十六章,一,6,注1),$p(x)=x-\alpha\in F[x]$,从而$p(x)$无重根. 所以α是F上可离元.

注　若$\alpha\in$域F,则称α为F上平凡可离元. 若$\alpha\overline{\in}$域F,且α是F上可离元,则称α为F上非平凡可离元.

3)　正确. 事实上,域F就是自身的可离扩域. 这是因为,F是F的代数扩域. $\forall\alpha\in F$,α

---

① 张禾瑞. 近世代数基础. 北京:高等教育出版社,1978. 174. 定理4.

② 同上. 149. 推论.

是 F 上可离元,从而 F 是 F 的可离扩域.

注 若 E 是 F 的可离扩域,$E\neq F$,则称 E 为 F 的真可离扩域.

11. 关于命题:设 F 是域,$f(x)$是 F 上的不可约多项式.

(i) 若 ch $F=\infty$,则 $f(x)$没有重根.

(ii) 若 ch $F=$素数 p,则

$$f(x)\text{ 有重根}\Leftrightarrow f(x)=g(x^p),\text{其中 } g(x)\in F[x]^{①}.$$

这里说明一下,$f(x)$是否有重根是在 $f(x)$的分裂域 E 中来谈的.

1) 为何:$g(x)(\in F[x])$在分裂域 E 中有重根$\Leftrightarrow g(x)$和 $g'(x)$在 $F[x]$中有次数$\geqslant 1$的公因子(即 $g(x),g'(x)$在 F 上不互素)?

2) 命题:设 $f(x)$在 F 上不可约,则

$$f(x)\text{ 有重根}\Leftrightarrow f'(x)=0$$

为何成立?

3) 证明(ii).

答 1) ($\Rightarrow$) 若 $g(x)$有重根,则 $g(x),g'(x)$的最大公因子 $d(x)(\in E[x])$的次数$\geqslant 1$.因 $d(x)$可由 $g(x),g'(x)$通过辗转相除法求出,而辗转相除法的基础是带余除法,只是对$g(x)$,$g'(x)$的系数($\in$域 F)进行加、减、乘、除的运算,从而每一步中出现的商式和余式都$\in F[x]$,所以 $d(x)\in F[x]$.即$\exists\, d(x)\in F[x]$,deg $d(x)\geqslant 1$,使得 $d(x)\mid g(x)$,且 $d(x)\mid g'(x)$.

($\Leftarrow$) 若 $g(x),g'(x)$在 $F[x]$中有次数$\geqslant 1$ 的公因子 $d(x)$,显然 $d(x)\in E[x]$,则$g(x)=d(x)h(x),g'(x)=d(x)k(x)$,其中 $h(x),k(x)\in E[x]$.因 E 是 $g(x)$在 F 上的分裂域,故 $d(x)=c_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_s)$,其中$\alpha_i\in E$,$1\leqslant s\leqslant \deg g(x)$.从而$x-\alpha_1\mid g(x)$,$x-\alpha_1\mid g'(x)$.所以 $g(x)$有重根 α_1.

2) ($\Rightarrow$) 若 $f(x)$有重根,则由本题 1),$f(x)$和 $f'(x)$在 $F[x]$中有次数$\geqslant 1$ 的公因子 $d(x)$.但因 $f(x)$在 F 上不可约,故 $f(x)$在 F 上只有平凡因子,而 $d(x)\neq$单位,于是 $d(x)$是 $f(x)$的相伴元.假设 $f'(x)\neq 0$,则 deg $f'(x)<$deg $f(x)=$deg $d(x)$,此与 $d(x)\mid f'(x)$矛盾.所以 $f'(x)=0$.

($\Leftarrow$) 若 $f'(x)=0$,则 $f(x)$和 $f'(x)$在 $F[x]$中有公因子 $f(x)$且 deg $f(x)\geqslant 1$,从而由本题 1),$f(x)$有重根.

3) ($\Rightarrow$) 因 $f(x)$有重根,故由本题 2),$f'(x)=0$.设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$,则 $f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1=0$,从而 $ia_i=0,i=0,1,2,\cdots,n$.若 $p\nmid i$,则 $i=q_ip+r_i$,其中 $0<r_i<p$.因 ch $F=p$,故 $ia_i=(q_ip+r_i)a_i=q_i(pa_i)+r_ia_i=\gamma_ia_i$,又 $ia_i=0$,于是 $r_ia_i=0$.因 $0<r_i<p$,ch $F=p$,故 $a_i=0$.即若 $p\nmid i$,则 $a_i=0$.所以

$$\begin{aligned}f(x)&=a_0+a_1x+\cdots+a_{p-1}x^{p-1}+a_px^p+a_{p+1}x^{p+1}+\cdots+\\&\quad a_{2p-1}x^{2p-1}+a_{2p}x^{2p}+a_{2p+1}x^{2p+1}+\cdots+a_nx^n\\&=a_0+a_px^p+a_{2p}(x^p)^2+\cdots+a_{tp}(x^p)^t=g(x^p),\end{aligned}$$

其中 $g(x)=a_0+a_px+a_{2p}x^2+\cdots+a_{tp}x^t\in F[x]$.即 $f(x)$可表成 F 上的 x^p 的多项式.

($\Leftarrow$) 因 $f(x)=g(x^p)$,故 $f(x)=b_m(x^p)^m+\cdots+b_1x^p+b_0$,从而 $f'(x)=$

① 张禾瑞.近世代数基础.北京:高等教育出版社,1978.175.引理 1.

$(pm)b_m x^{pm-1}+\cdots+pb_1x^{p-1}$. 因 ch $F=p$,故 $f'(x)=0$. 由本题 2),$f(x)$有重根.

注　1)　由本题 1)知,$g(x)(\in F[x])$在 F 的扩域中有无重根的问题可以直接在 F 上来判别.

2)　本命题给出了域 F 上不可约多项式在分裂域中有无重根的判别方法.

例　用 a 表示 $\mathbb{Z}_3$ 中的元$[a]$. $f(x)=x^3+2x+1(\in\mathbb{Z}_3[x])$无重根.

事实上,因 ch $\mathbb{Z}_3=3$,故 $f'(x)=3x^2+2=2$,从而 $f(x)$,$f'(x)$互素. 由本题 1),$f(x)$无重根.

另一证法,因 $f(x)$在 $\mathbb{Z}_3$中无根,故 $f(x)$在 $\mathbb{Z}_3$上不可约. 又 ch $\mathbb{Z}_3=3$,$f(x)\neq g(x^3)$,从而由本命题,$f(x)$无重根.

12. 关于命题:设 $F=\Delta(\xi)$,其中 Δ 是特征为 3 的素域,ξ 是 Δ 上超越元.

1)　为何元 $\xi(\in F)$不是 F 的某一元的 3 次幂?

2)　为何 F 有不可离扩域?

3)　为何 $x^2-\xi(\in F[x])$在 F 上不可约?

4)　为何 $x^2-\xi$ 在分裂域中没有重根?

5)　为何有 F 上非平凡可离元[①]?

答　1)　ξ 不是 F 的某一元的 3 次幂. 不然,若 $\exists b=\dfrac{a_0+a_1\xi+\cdots+a_n\xi^n}{b_0+b_1\xi+\cdots+b_m\xi^m}\in F$,其中 $a_i,b_j\in\Delta$,$b_0+b_1\xi+\cdots+b_m\xi^m\neq0$,使得 $\xi=b^3$. 则

$$\xi(b_0+b_1\xi+\cdots+b_m\xi^m)^3=(a_0+a_1\xi+\cdots+a_n\xi^n)^3.$$

因 ch $F=3$,故由第十章,三,4,3),

$$\xi({b_0}^3+b_1^3\xi^3+\cdots+b_m^3\xi^{3m})=a_0^3+a_1^3\xi^3+\cdots+a_n^3\xi^{3n},$$

即

$$a_0^3-b_0^3\xi+a_1^3\xi^3-b_1^3\xi^4+\cdots+a_n^3\xi^{3n}-b_m^3\xi^{3m+1}=0,$$

其中显然 $3n\neq3m+1$. 因 ξ 是 Δ 上超越元,故 $b_0^3=b_1^3=\cdots=b_m^3=0$,即 $b_0=b_1=\cdots=b_m=0$,此与 $b_0+b_1\xi+\cdots+b_m\xi^m\neq0$ 矛盾. 所以 ξ 不是 F 的某一元的 3 次幂.

2)　因 ch $F=$ch$\Delta=3$,ξ 不是 F 的某一元的 3 次幂,故 F 有不可离扩域[②].

3)　域 Δ 上的 ξ 的多项式环 $\Delta[\xi]$是唯一分解环,$x^2-\xi\in\Delta[\xi][x]$. ξ 是环 $\Delta[\xi]$的素元. 这是因为,ξ 是 Δ 上超越元(即未定元),从而 $\xi\neq0$,$\xi\overline{\in}\Delta$,于是 $\xi\neq$单位. 若 $\xi=h(\xi)k(\xi)$,其中 $h(\xi)$,$k(\xi)\in\Delta[\xi]$,由第十一章,四,1,10),$h(\xi)$,$k(\xi)$中必有一个是单位,由第十四章,一,6,ξ 无真因子. 所以 ξ 是环 $\Delta[\xi]$的素元. 显然 $\xi\nmid1$,$\xi\mid\xi$,但 $\xi^2\nmid\xi$,又 $x^2-\xi$ 在 $\Delta[\xi]$中无真因子. 于是由第十五章,四,13,艾森斯坦因不可约性判别准则,$x^2-\xi$ 在 $\Delta[\xi]$上不可约,从而 $x^2-\xi$ 在 $\Delta[\xi]$的商域 $\Delta(\xi)=F$ 上也不可约.

4)　设 $f(x)=x^2-\xi$,则 $f'(x)=2x$. 因 ch $F=3$,故 $f'(x)\neq0$,由第十七章,一,11,2),$x^2-\xi$在分裂域中没有重根.

5)　因 $f(x)=x^2-\xi(\in F[x])$在 F 上不可约,故由第十六章,二,4,$\exists F$ 的单代数扩域 $E=F(\alpha)$,其中 α 在 F 上极小多项式为 $f(x)=x^2-\xi$. 因 $f(x)$没有重根,故 α 是 F 上可离

---

① 张禾瑞. 近世代数基础. 北京:高等教育出版社,1978. 177. 例.

② 同上. 176. 引理 2.

元. 又 $\alpha \overline{\in} F$. 否则,若 $\alpha \in F$,而 α 是 $f(x)$ 的根,从而 $f(x)$ 在 F 上可约,矛盾. 于是 $\alpha \overline{\in} F$. 所以 α 是 F 上非平凡可离元.

注 1) 若 p 是素数,域 F 的特征是素数 q,但 $p \neq q$,则

多项式 $x^p - b$ 在 F 上不可约 $\Leftrightarrow b$ 不是 F 的某一元的 p 次幂.

2) 类似地有下面命题:设 $F = \Delta(\xi)$,其中 Δ 是特征为 p 的素域,ξ 是 Δ 上超越元,则

(i) 元 $\xi(\in F)$ 不是 F 的某一元的 p 次幂.

(ii) $x^p - \xi(\in F[x])$ 在 F 上不可约.

(iii) $x^p - \xi(\in F[x])$ 在分裂域中有重根.

(iv) $F(\alpha)$ 是 F 的不可离扩域,其中 α 是 $x^p - \xi$ 的根.

(V) 在 $\Delta(\alpha)$ 上分解 $x^p - \xi$ 为不可约因子的积.

事实上,(i) 用本题 1)的证法可证.

(ii) 用本题 3)的证法可证. 下面再给出一个证法. 假设 $f(x) = x^p - \xi$ 在 F 上不是不可约,又 $f(x) \neq 0$,$f(x) \neq$ 单位,则 $f(x)$ 在 F 上可约,由第十五章,一,4,注 3),$f(x) = g(x)h(x)$,其中 $g(x), h(x) \in F[x]$,$0 < \deg g(x) = s < \deg f(x) = p$,$0 < \deg h(x) < \deg f(x) = p$. 不妨假设 $g(x)$ 的最高系数为 1. 设 E 是 $f(x)$ 在 F 上的分裂域,$\alpha(\in E)$ 是 $f(x)$ 的一个根,即 $f(\alpha) = 0$,则 $\alpha^p = \xi$. 因 $\mathrm{ch}\, E = p$,故由第十章,三,4,1),

$$f(x) = x^p - \xi = x^p - \alpha^p = (x - \alpha)^p = g(x)h(x),$$

从而 $g(x) = (x-\alpha)^s = x^s - s\alpha x^{s-1} + \cdots + (-1)^s\alpha^s$. 因 $g(x) \in F[x]$,故系数 $(-1)^s\alpha^s \in F$,即 $\alpha^s \in F$. 因在 $\mathbb{Z}$ 中 s, p 互素,故 $\exists u, v \in \mathbb{Z}$,使得 $su + pv = 1$. 又因 $\alpha^p = \xi \in F$,故 $\alpha = \alpha^{su+pv} = (\alpha^s)^u \cdot (\alpha^p)^v \in F$. 即在 F 中有元 α,使 $\alpha^p = \xi$,此与(i)矛盾. 所以 $f(x) = x^p - \xi$ 在 F 上不可约.

(由此证明知:设 F 是域,$\mathrm{ch}\, F =$ 素数 p,$x^p - \xi \in F[x]$. 若 ξ 不是 F 的某一元的 p 次幂,则 $x^p - \xi$ 在 F 上不可约.)

(iii) 因 $\mathrm{ch}\, F = p$,故 $f'(x) = px^{p-1} = 0$,从而由第十七章,一,11,2),$f(x) = x^p - \xi$ 在分裂域中有重根.

(iv) $\alpha \in F(\alpha)$,又由(ii),(iii),α 在 F 上极小多项式 $x^p - \xi$ 有重根,从而 α 不是 F 上可离元. 所以 $F(\alpha)$ 是 F 的不可离扩域,且 $F(\alpha) = \Delta(\alpha)$. 事实上,显然 $\Delta(\alpha) \subset F(\alpha)$. 反之,因 $x^p - \xi$ 是 α 在 F 上极小多项式,故 $\xi = \alpha^p \in \Delta(\alpha)$,从而 $F(\alpha) = \Delta(\xi)(\alpha) \subset \Delta(\alpha)$. 所以 $F(\alpha) = \Delta(\xi)(\alpha) = \Delta(\alpha)$.

(V) 因 $x^p - \xi$ 是 α 在 F 上极小多项式,故 $\alpha^p = \xi$. 又 $\mathrm{ch}\, \Delta(\alpha) = p$,从而 $x^p - \xi = x^p - \alpha^p = (x - \alpha)^p$.

13. 关于命题:设 F 是特征为 p 的域,则

$$\alpha \text{ 是 } F \text{ 上可离元} \Leftrightarrow F(\alpha) = F(\alpha^p)^{①}.$$

1) 设 α 是 F 上可离元,为何 α 是 $F(\alpha^p)$ 上可离元?

2) 为何 α 在 $F(\alpha^p)$ 上极小多项式 $h(x)$ 可以在 E 里写成 $(x-\alpha)^m$,$1 \leqslant m \leqslant p$?

3) 为何由 $\deg f(x) \neq \deg g(x)$,得 $F(\alpha) \neq F(\alpha^p)$?

答 1) 因 α 是 F 上可离元,故 α 是 F 上代数元,又 $F \subset F(\alpha^p)$,从而 α 也是 $F(\alpha^p)$ 上代

① 张禾瑞. 近世代数基础. 北京:高等教育出版社,1978. 177. 引理 3.

数元. 于是有 α 在 F 上极小多项式 $f(x)$ 和 α 在 $F(\alpha^p)$ 上极小多项式 $h(x)$. 由第十六章,一,6,注 7),$h(x)\mid f(x)$. 因 α 是 F 上可离元,故 $f(x)$ 无重根,因此 $h(x)$ 也无重根. 所以 α 是 $F(\alpha^p)$ 上可离元.

2)　因 α 是 $x^p-\alpha^p$ 的根,故由第十六章,一,6,2),(1),$h(x)\mid x^p-\alpha^p$. 因 ch $E=p$,故 $x^p-\alpha^p=(x-\alpha)^p$,从而 $h(x)=(x-\alpha)^m$ 且 $m\neq 0$,不然,$m=0$ 时,$h(x)=1$,此与 $h(x)$ 不可约矛盾. 于是 $1\leqslant m\leqslant p$.

3)　因 $(F(\alpha):F)=\deg f(x)$,$(F(\alpha^p):F)=\deg g(x)$,今 $\deg f(x)\neq\deg g(x)$,故 $(F(\alpha):F)\neq(F(\alpha^p):F)$,即 $F(\alpha)$ 与 $F(\alpha^p)$ 看作同一域 F 上的向量空间时,维数不等,所以 $F(\alpha)\neq F(\alpha^p)$.

注　1)　设 E 是域 F 的扩域,若 α 是 F 上可离元,则 α 也是 E 上可离元. 理由同本题 1).

2)　若 $E=F(\alpha_1,\alpha_2)$ 是域 F 的可离扩域,则 E 是 $F(\alpha_1)$ 的可离扩域. 事实上,$\forall\alpha\in E$,因 E 是 F 的可离扩域,故 α 是 F 上可离元,从而由注 1),α 也是 $F(\alpha_1)$ 上可离元,所以 E 是 $F(\alpha_1)$ 的可离扩域.

推广来说,若 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_k)$ 是域 F 的可离扩域,则 E 是 $F(\alpha_i)(1\leqslant i\leqslant k)$ 的可离扩域.

14. 关于命题:设 β 是域 F 上可离元. 若 α 是 $E=F(\beta)$ 上可离元,则 α 是 F 上可离元[①].

1)　为何 ch $F=\infty$ 时,命题成立?

2)　为何 $g(x)=h(x)$?

3)　为何 $F(\alpha)=F(\alpha^p)$?

答　1)　因 α 是 E 上可离元,当然 α 是 E 上代数元,故 α 在 E 的代数扩域 $E(\alpha)$ 中. 又 E 是 F 的代数扩域,从而由第十六章,二,6,注 3),代数扩域的传递性,$E(\alpha)$ 是 F 的代数扩域. 今 ch $F=\infty$,则 $E(\alpha)$ 是 F 的可离扩域. 所以 α 是 F 上的可离元.

2)　已知 $h(x)\mid(g(x))^p$. 因 $g(x)$ 是 β 在 $F(\alpha)$ 上极小多项式,故 $g(x)$ 是 $F(\alpha)$ 上的不可约多项式,从而 $h(x)=(g(x))^m$,$1\leqslant m\leqslant p$. 又 β 是 F 上可离元,由第十七章,一,13,β 也是 $F(\alpha^p)$ 上可离元,于是 β 在 $F(\alpha^p)$ 上极小多项式 $h(x)$ 没有重根,所以 $m=1$,即 $h(x)=g(x)$.

3)　由 $h(x)=g(x)$,有

$$(F(\alpha^p)(\beta):F(\alpha^p))=\deg h(x)=\deg g(x)=(F(\alpha)(\beta):F(\alpha)).$$

由 $F(\beta,\alpha)=F(\beta,\alpha^p)$,有 $(F(\alpha,\beta):F(\alpha^p))=(F(\alpha,\beta):F(\alpha))$. 又

$$(F(\alpha,\beta):F)=(F(\alpha,\beta):F(\alpha^p))(F(\alpha^p):F),$$

$$(F(\alpha,\beta):F)=(F(\alpha,\beta):F(\alpha))(F(\alpha):F),$$

从而 $(F(\alpha^p):F)=(F(\alpha):F)$. 但 $F(\alpha^p)\subset F(\alpha)$,所以 $F(\alpha)=F(\alpha^p)$.

注　由第十七章,一,13,注 1),该命题的逆命题成立. 即:设 β 是域 F 上可离元,若 α 是 F 上可离元,则 α 是 $E=F(\beta)$ 上可离元.

15. 关于命题:若 α,β 是域 F 上可离元,则 $F(\alpha,\beta)$ 是 F 的可离扩域[②].

---

① 张禾瑞. 近世代数基础. 北京:高等教育出版社,1978. 178. 引理 4.

② 同上. 179. 定理 3.

1) $\forall \gamma(\in F(\alpha,\beta))$为何是$F(\alpha,\beta)$上可离元?

2) 若域F上有非平凡可离元,为何F有真可离扩域?

答 1) 由第十七章,一,10,2)知,$F(\alpha,\beta)$中元都是$F(\alpha,\beta)$上可离元.

2) 取$\alpha=\beta$是F上非平凡可离元,即$\alpha \overline{\in} F$.从而$F(\alpha,\beta)=F(\alpha)\neq F$.于是由该命题,$F(\alpha)$是$F$的真可离扩域.

注 1) 特征$=\infty$的域的任何代数扩域都是可离扩域.又有限域的任何代数扩域都是可离扩域.由该命题,域F上只要有非平凡可离元,则F必有真可离扩域.因而可离扩域出现的可能性很大,多数重要且有兴趣的扩域都是可离扩域.因为可离扩域有一些特殊的较好的结果.比如,域F的可离扩域E的自同构的个数恰是$(E:F)$.证略.

2) 设F是域,ch $F=$素数p,则

(i) F上只有平凡可离元

$\Leftrightarrow$(ii) F上每个次数大于1的,不是$g(x^p)$形状的多项式都可约

$\Leftrightarrow$(iii) F没有真可离扩域.

事实上,(i)$\Rightarrow$(ii),假设F上有一个次数大于1的,不是$g(x^p)$形状的多项式$f(x)$不可约,不妨令$f(x)$的最高系数等于1.由第十六章,二,4,$\exists F$的单代数扩域$F(\alpha)$,而α在F上极小多项式为$f(x)$.由第十七章,一,11,$f(x)$没有重根.于是α是F上可离元,且$\alpha \overline{\in} F$(不然,若$\alpha\in F$,则α在F上极小多项式$f(x)=x-\alpha$是一次的,矛盾).所以α是F上非平凡可离元,与已知矛盾.因此(ii)成立.

(ii)$\Rightarrow$(iii),假设F有真可离扩域E,则$E\supsetneqq F$.于是$\exists\alpha\in E,\alpha \overline{\in} F$,$\alpha$是$F$上可离元,从而$\exists\alpha$在$F$极小多项式$p(x)$且$\deg p(x)>1$,$p(x)$没有重根.由第十七章,一,11,$p(x)$不是$g(x^p)$形状的多项式,但$p(x)$不可约,此与已知矛盾.所以$F$没有真可离扩域.

(iii)$\Rightarrow$(i),假设F上有非平凡可离元,由本题2),F有真可离扩域,矛盾.所以(i)成立.

16. 证明命题:若α,β是域F上可离元,则$\alpha\pm\beta,\alpha\beta,\dfrac{\alpha}{\beta}(\beta\neq 0)$也是$F$上可离元①.

证 利用第十七章,一,15,仿第十六章,一,11,1)可证.

注 设E是域F的代数扩域,$I=\{\alpha\in E \mid \alpha$是$F$上可离元$\}$,则$I$是$E$的子域,且$I$是$F$的可离扩域.仿第十六章,一,11,2)可证.

17. 关于命题:设E是域F的有限可离扩域(既是有限扩域,又是可离扩域),则E是F的单扩域②.

1) 若F是有限域,为何E也是有限域?

2) 若F是有限域,为何$E=\Delta(\alpha)=F(\alpha)$?

3) 要证明F的可离扩域$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$是$F$的单扩域,为何只需证明$F$的可离扩域$F(\beta,\gamma)$是$F$的单扩域?

4) 为何$s\cdot(t-1)$个方程$\beta_i+x\gamma_j=\beta_1+x\gamma_1(i=1,2,\cdots,s;j=2,3,\cdots,t)$中的每一个方程在$F$里最多有一个解?

答 1) 因E是F的有限扩域,故E是F上有限维(n维)空间.设$\alpha_1,\alpha_2,\cdots,\alpha_n$是$E$在

---

① 张禾瑞.近世代数基础.北京:高等教育出版社,1978.179.推论.

② 同上.180.定理4.

F 上的一个基，则 $\forall\alpha\in E$，α 可唯一写成 $\alpha=\sum_{i=1}^{n}a_i\alpha_i$，$a_i\in F$. 因 F 是有限域，故 F 中的元 a_i 只有有限个，从而 E 也是有限域.

（由第十六章，三，1，15），F 的有限扩域 E 未必是有限域，但进一步 F 是有限域时，E 也是有限域.）

2） 由第十七章，一，9，$E=\Delta(\alpha)$，其中 Δ 是 E 的素子域. 因 F 是 E 的子域，故由第十六章，四，1，1），$\Delta\subset F$，从而 $\Delta(\alpha)\subset F(\alpha)$；反之，因 $F\subset E$，$\alpha\in E$，又 $F(\alpha)$ 是含 F，α 的最小域，故 $F(\alpha)\subset E=\Delta(\alpha)$. 所以 $E=\Delta(\alpha)=F(\alpha)$.

3） 如果已经证明了 F 的可离扩域 $F(\beta,\gamma)$ 是 F 的单扩域. 今 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是 F 的可离扩域. 要证 E 是 F 的单扩域. 对 n 作数学归纳法. $n=2$ 时，已知命题成立. 假定 k 时，命题成立. 下面看 $k+1$ 时，设 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_k,\alpha_{k+1})=F(\alpha_{k+1})(\alpha_1,\alpha_2,\cdots,\alpha_k)$ 是 F 的可离扩域，则由第十七章，一，13，注 2），E 是 $F(\alpha_{k+1})$ 的可离扩域. 由归纳假定，E 是 $F(\alpha_{k+1})$ 的单扩域，即 $E=F(\alpha_{k+1})(\delta)=F(\alpha_{k+1},\delta)$，又 E 是 F 的可离扩域，由已知条件，E 是 F 的单扩域. 所以依归纳原理，命题成立.

4） 因为 $F(\beta,\gamma)$ 是 F 的可离扩域，故 γ 是 F 上可离元，从而 γ 在 F 上极小多项式 $g(x)$ 没有重根，于是 $\gamma_j\neq\gamma_1$，即 $\gamma_j-\gamma_1\neq0$，$j=2,3,\cdots,t$. 所以 $\beta_i+x\gamma_j=\beta_1+x\gamma_1$ 中每个方程都是 L 上一次方程，因此在 F 里最多有一个解.

注 1） 有限域 F 的任一有限扩域 E 是 F 的单代数扩域. 事实上，由第十六章，一，10，E 是 F 的代数扩域，从而 E 是 F 的可离扩域. 由该命题，E 是 F 的单代数扩域.

2） 特征为 ∞ 的域 F 的有限扩域 E 是 F 的单扩域. 易证.

例 数域的有限扩域是单扩域. 因数域的特征为 ∞.

例 设 F 是数域，则 $f(x)(\in F[x])$ 在 F 上的分裂域 E 是 F 的单扩域. 因 E 是特征为 ∞ 的域 F 的有限扩域.

3） 由于域 F 的有限可离扩域是单扩域，因此大大简化了有限可离扩域的研究，这是因为单扩域 $F(\alpha)$ 的结构是十分清楚、非常简单的. 例如它的元可唯一表成 α 的多项式 $\sum_{i=0}^{n-1}a_i\alpha^i$ 的形式，其中 $n=(F(\alpha):F)$. 所以这个扩域的构造及同构都较易掌握. 由该命题，也显示出单代数扩域的重要性.

4） 由该命题的证明知，域 F 的有限可离扩域 $F(\beta,\gamma)$ 是单扩域 $F(\theta)$，其中 $\theta=\beta+c\gamma$，而 $c\neq\dfrac{\beta_i-\beta_1}{\gamma_1-\gamma_j}$，这里 $\beta_1=\beta$，$\gamma_1=\gamma$，$j\neq1$，$j=2,3,\cdots,t$，$i=1,2,\cdots,s$，β_i 是 β 在 F 上极小多项式的根，γ_j 是 γ 在 F 上极小多项式的根.

例 (i) $\mathbf{Q}$ 的有限扩域 $\mathbf{Q}(\sqrt{2},\sqrt{3})$ 是单扩域 $\mathbf{Q}(\theta)$，求出 θ.

$\beta=\sqrt{2}$ 在 $\mathbf{Q}$ 上极小多项式是 x^2+2，其根为 $\beta=\beta_1=\sqrt{2}$，$\beta_2=-\sqrt{2}$. $\gamma=\sqrt{3}$ 在 $\mathbf{Q}$ 上极小多项式是 x^2-3，其根为 $\gamma=\gamma_1=\sqrt{3}$，$\gamma_2=-\sqrt{3}$. $c\neq\dfrac{\beta_1-\beta_1}{\gamma_1-\gamma_2}=0$，$c\neq\dfrac{\beta_2-\beta_1}{\gamma_1-\gamma_2}=\dfrac{-\sqrt{2}-\sqrt{2}}{\sqrt{3}-(-\sqrt{3})}=-\dfrac{\sqrt{2}}{\sqrt{3}}$. 取 c 为除 0 外的任意一个有理数都是可以的. 今取 $c=1$，此时 $\theta=\beta+c\gamma=\sqrt{2}+\sqrt{3}$，即 $\mathbf{Q}(\sqrt{2},\sqrt{3})=\mathbf{Q}(\sqrt{2}+\sqrt{3})$. 也可取 $c=-1$，此时 $\mathbf{Q}=\sqrt{2}-\sqrt{3}$，即 $\mathbf{Q}(\sqrt{2},\sqrt{3})=\mathbf{Q}(\sqrt{2}-\sqrt{3})$. 同理，$\mathbf{Q}(\sqrt{2},\sqrt{3})=\mathbf{Q}(\sqrt{2}+7\sqrt{3})=\mathbf{Q}(\sqrt{2}-10\sqrt{3})$，等等.

(ii) 求出$\sqrt{2}+\sqrt{3}$在$\mathbb{Q}$上极小多项式.

设$\theta=\sqrt{2}+\sqrt{3}$,则$\theta^2=5+2\sqrt{6}$,$(\theta^2-5)^2=(2\sqrt{6})^2$,从而$\theta^4-10\theta^2+1=0$. 因此$\theta$是$\mathbb{Q}$上多项式$p(x)=x^4-10x^2+1$的根. 因$\sqrt{3}$在$\mathbb{Q}(\sqrt{2})$上极小多项式是$x^2-3$,$\sqrt{2}$在$\mathbb{Q}$上极小多项式是$x^2-2$. 故

$$(\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q})=(\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q})=(\mathbb{Q}(\sqrt{2})(\sqrt{3}):\mathbb{Q}(\sqrt{2}))(\mathbb{Q}(\sqrt{2}):\mathbb{Q})=2\cdot 2=4.$$

所以$p(x)=x^4-10x^2+1$是$\sqrt{2}+\sqrt{3}$在$\mathbb{Q}$上极小多项式.

另一求法,

$$\begin{aligned} p(x)&=[x-(\sqrt{2}+\sqrt{3})][x-(\sqrt{2}-\sqrt{3})][x-(-\sqrt{2}+\sqrt{3})][x-(-\sqrt{2}-\sqrt{3})] \\ &=x^4-10x^2+1, \end{aligned}$$

显然$\sqrt{2}+\sqrt{3}$是$p(x)$的一个根. 因$\sqrt{2}+\sqrt{3},\sqrt{2}-\sqrt{3},-\sqrt{2}+\sqrt{3},-\sqrt{2}-\sqrt{3}\,\overline{\in}\,\mathbb{Q}$,故$p(x)$在$\mathbb{Q}$上没有一次因子,即$p(x)$在$\mathbb{Q}$上不能写成一次因子和三次因子的积. 因$p(x)$中任意两个一次因子的积都$\overline{\in}\,\mathbb{Q}[x]$,故$p(x)$不能写成$\mathbb{Q}$上两个二次因子的积. 所以$p(x)$在$\mathbb{Q}$上不可约. 于是$p(x)$是$\sqrt{2}+\sqrt{3}$在$\mathbb{Q}$上极小多项式.

(iii) 求出$\mathbb{Q}(\sqrt{2}+\sqrt{3})$在$\mathbb{Q}$上的一个基:

$1,\sqrt{2}+\sqrt{3},(\sqrt{2}+\sqrt{3})^2,(\sqrt{2}+\sqrt{3})^3$是$\mathbb{Q}(\sqrt{2}+\sqrt{3})$在$\mathbb{Q}$上的一个基.

另一求法,因$\mathbb{Q}(\sqrt{2}+\sqrt{3})=\mathbb{Q}(\sqrt{2},\sqrt{3})$在$\mathbb{Q}(\sqrt{2})$上的一个基是$1,\sqrt{3}$;$\mathbb{Q}(\sqrt{2})$在$\mathbb{Q}$上的一个基是$1,\sqrt{2}$,故由第十六章,一,9 中命题的证明知$\mathbb{Q}(\sqrt{2}+\sqrt{3})$在$\mathbb{Q}$上的一个基是$1,\sqrt{2},\sqrt{3},\sqrt{6}$.

(iv) 直接证明$\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

证一 令$\theta=\sqrt{2}+\sqrt{3}$,则$(\sqrt{2}-\theta)^2=3$,即$2+\theta^2-2\theta\sqrt{2}=3$,于是$\sqrt{2}=\dfrac{1-\theta^2}{-2\theta}\in\mathbb{Q}(\theta)$. 同理$\sqrt{3}\in\mathbb{Q}(\theta)$. 因而$\mathbb{Q}(\sqrt{2},\sqrt{3})\subset\mathbb{Q}(\theta)$;反之,显然成立. 所以$\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

证二 显然$\mathbb{Q}(\sqrt{2}+\sqrt{3})$是$\mathbb{Q}(\sqrt{2},\sqrt{3})$的子域.

$$\begin{aligned} (\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q})&=(\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2}+\sqrt{3}))(\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}) \\ &=(\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2}+\sqrt{3}))\cdot 4. \end{aligned}$$

又$(\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q})=4$,从而$(\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2}+\sqrt{3}))=1$. 由第十六章,一,12,$\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

证三 因$\sqrt{2}+\sqrt{3}$在$\mathbb{Q}$上极小多项式是x^4-10x^2+1,故$(\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q})=4$. 又$(\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q})=4$. $\mathbb{Q}(\sqrt{2},\sqrt{3})$是$\mathbb{Q}(\sqrt{2}+\sqrt{3})$的扩域. 从而由第十六章,三,1,18),①,$\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

证四 由$\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$,$(\sqrt{2}+\sqrt{3})^{-1}=\dfrac{1}{\sqrt{2}+\sqrt{3}}=-(\sqrt{2}-\sqrt{3})\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$,$\sqrt{2}-\sqrt{3}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$. 因此$\sqrt{2}=\dfrac{\sqrt{2}+\sqrt{3}+\sqrt{2}-\sqrt{3}}{2}$,$\sqrt{3}=\dfrac{\sqrt{2}+\sqrt{3}-\sqrt{2}+\sqrt{3}}{2}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$,于是$\mathbb{Q}(\sqrt{2},\sqrt{3})\subset\mathbb{Q}(\sqrt{2}+\sqrt{3})$;反之也成立. 从而$\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

证五　显然$\mathbb{Q}(\sqrt{2}+\sqrt{3})\subset\mathbb{Q}(\sqrt{2},\sqrt{3})$；反之，设$\theta=\sqrt{2}+\sqrt{3}$，则$\theta^3=11\sqrt{2}+9\sqrt{3}$. 从而$\sqrt{2}=-\frac{9}{2}\theta+\frac{1}{2}\theta^3$，$\sqrt{3}=\frac{11}{2}\theta-\frac{1}{2}\theta^3\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$. 于是$\mathbb{Q}(\sqrt{2},\sqrt{3})\subset\mathbb{Q}(\sqrt{2}+\sqrt{3})$. 所以$\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

二、典型问题分析

1. 证明：有理数域$\mathbb{Q}$上多项式x^4+1的分裂域是一个单扩域$\mathbb{Q}(\alpha)$，其中α是x^4+1的一个根.

证　在复数域$\mathbb{C}$上，$x^4+1=(x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1)$，因此$x^4+1$在$\mathbb{C}$里的4个根是

$$\alpha=\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}\mathrm{i}\quad,\quad\alpha_1=\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}\mathrm{i},$$

$$\alpha_2=-\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}\mathrm{i}\quad,\quad\alpha_3=-\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}\mathrm{i}.$$

因$\alpha_1=\alpha^{-1}(\alpha\alpha_1=\frac{1}{2}+\frac{1}{2}=1)$(即$\alpha_1=-\alpha^3$)，$\alpha_2=-\alpha^{-1}$(即$\alpha_1=\alpha^3$)，$\alpha_3=-\alpha$，故$x^4+1$在$\mathbb{Q}$上的分裂域是$\mathbb{Q}(\alpha,\alpha_1,\alpha_2,\alpha_3)=\mathbb{Q}(\alpha)$，其中$\alpha$是$x^4+1$的一个根.

注　1)　$\mathbb{Q}(\alpha)=\mathbb{Q}\left(\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}\mathrm{i}\right)=\mathbb{Q}(\sqrt{2},\mathrm{i})$. 事实上，因$\sqrt{2}=2(\alpha+\alpha_1)\in\mathbb{Q}(\alpha)$，$\mathrm{i}=\frac{\alpha+\alpha_2}{\sqrt{2}}\in\mathbb{Q}(\alpha)$，故$\mathbb{Q}(\sqrt{2},\mathrm{i})\subset\mathbb{Q}(\alpha)$；反之显然成立. 所以$\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{2},\mathrm{i})$. 显然$(\mathbb{Q}(\alpha):\mathbb{Q})=(\mathbb{Q}(\sqrt{2})(\mathrm{i}):\mathbb{Q}(\sqrt{2}))(\mathbb{Q}(\sqrt{2}):\mathbb{Q})=2\cdot2=4$.

2)　α在$\mathbb{Q}$上极小多项式是x^4+1. 事实上，α是x^4+1的根. 用$x+1$代x，得$(x+1)^4+1=x^4+4x^3+6x^2+4x+2$. 2是素数，$2\nmid1$，$2\mid4$，$2\mid6$，$2\mid2$，但$2^2\nmid2$. 又$(x+1)^4+1$在$\mathbb{Z}$中无真因子，从而由第十五章，四，13，艾森斯坦因不可约性判别准则，$(x+1)^4+1$在$\mathbb{Q}$上不可约. 由第十五章，四，13，注2)，x^4+1在$\mathbb{Q}$上也不可约. 所以x^4+1是α在$\mathbb{Q}$上极小多项式. 或由$(\mathbb{Q}(\alpha):\mathbb{Q})=4$亦可知此结论.

3)　实际上，$\mathbb{Q}(\alpha)=\mathbb{Q}(\alpha_1)=\mathbb{Q}(\alpha_2)=\mathbb{Q}(\alpha_3)$.

2. 令$\mathbb{Q}$是有理数域，x^3-a是$\mathbb{Q}$上一个不可约多项式，而α是x^3-a的一个根. 证明：$\mathbb{Q}(\alpha)$不是x^3-a在$\mathbb{Q}$上的分裂域.

证一　假设$\mathbb{Q}(\alpha)$是x^3-a在$\mathbb{Q}$上的分裂域，则x^3-a的全部三个根$\alpha,\alpha\omega,\alpha\omega^2\in\mathbb{Q}(\alpha)$，其中$\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}$是一个三次单位原根. $\alpha\neq0$(不然，若$\alpha=0$，则$\alpha^3-a=-a=0$，即$a=0$，此与x^3-a在$\mathbb{Q}$上不可约矛盾)，从而$\exists\,\alpha^{-1}\in$域$\mathbb{Q}(\alpha)$，使得$\alpha^{-1}(\alpha\omega)=\omega\in\mathbb{Q}(\alpha)$. 又$\mathbb{Q}$的单代数扩域$\mathbb{Q}(\alpha)$是$\mathbb{Q}$的有限扩域，由第十六章，一，9，注1)，$(\mathbb{Q}(\omega):\mathbb{Q})\mid(\mathbb{Q}(\alpha):\mathbb{Q})$. 因$\omega$在$\mathbb{Q}$上极小多项式是$x^2+x+1$，故$(\mathbb{Q}(\omega):\mathbb{Q})=2$. 而$\alpha$在$\mathbb{Q}$上极小多项式是$x^3-a$，故$(\mathbb{Q}(\alpha):\mathbb{Q})=3$，于是$2\mid3$，矛盾. 所以$\mathbb{Q}(\alpha)$不是$x^3-a$在$\mathbb{Q}$上的分裂域.

证二 因$\sqrt[3]{a}$是x^3-a的一个根，故x^3-a的三个根是$\sqrt[3]{a},\omega\sqrt[3]{a},\omega^2\sqrt[3]{a}$，其中$\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i},\omega^3=1$. 于是$x^3-a$在$\mathbb{Q}$上的分裂域是$E=\mathbb{Q}(\sqrt[3]{a},\omega\sqrt[3]{a},\omega^2\sqrt[3]{a})$. 因$\omega=(\omega\sqrt[3]{a})(\sqrt[3]{a})^{-1}\in E$，故$\mathbb{Q}(\sqrt[3]{a},\omega)\subset E$；反之，显然$E\subset\mathbb{Q}(\sqrt[3]{a},\omega)$，所以$E=\mathbb{Q}(\sqrt[3]{a},\omega\sqrt[3]{a},\omega^2\sqrt[3]{a})=\mathbb{Q}(\sqrt[3]{a},\omega)$. 因$E$是$\mathbb{Q}$的有限扩域，故由第十六章，一，9，

$$(E:\mathbb{Q})=(\mathbb{Q}(\sqrt[3]{a},\omega):\mathbb{Q})=(\mathbb{Q}(\sqrt[3]{a})(\omega):\mathbb{Q}(\sqrt[3]{a}))(\mathbb{Q}(\sqrt[3]{a}):\mathbb{Q}).$$

因$\omega\overline{\in}\mathbb{Q}(\sqrt[3]{a})$，故$\omega$在$\mathbb{Q}(\sqrt[3]{a})$上极小多项式不会是一次的，又$\omega$是$\mathbb{Q}(\sqrt[3]{a})$上多项式$x^2+x+1$的根，从而$(\mathbb{Q}(\sqrt[3]{a})(\omega):\mathbb{Q}(\sqrt[3]{a}))=2$. 因$\sqrt[3]{a}$在$\mathbb{Q}$上极小多项式是$x^3-a$，故$(\mathbb{Q}(\sqrt[3]{a}):\mathbb{Q})=3$. 所以$(E:\mathbb{Q})=2\cdot3=6$. 但因$\alpha$在$\mathbb{Q}$上极小多项式也是$x^3-a$，故$(\mathbb{Q}(\alpha):\mathbb{Q})=3$. 于是$(E:\mathbb{Q})\neq(\mathbb{Q}(\alpha):\mathbb{Q})$，因此$\mathbb{Q}(\alpha)\neq E$，即$\mathbb{Q}(\alpha)$不是$x^3-a$在$\mathbb{Q}$上的分裂域.

3. 令$p_1(x),p_2(x),\cdots,p_m(x)$是域$F$上$m$个最高系数为1的不可约多项式. 证明：存在$F$的一个有限扩域$F(\alpha_1,\alpha_2,\cdots,\alpha_m)$，其中$\alpha_i$在$F$上的极小多项式是$p_i(x)$.

证一 设α_i是$p_i(x)$的一个根，$i=1,2,\cdots,m$. 因$p_i(x)\in F[x]$，$p_i(x)\neq0$，故α_i是F上代数元. 从而$F(\alpha_1,\alpha_2,\cdots,\alpha_m)$是$F$的有限扩域，且$\alpha_i$在$F$上极小多项式是$p_i(x)$.

证二 作$f(x)=p_1(x)p_2(x)\cdots p_m(x)$. 由第十七章，一，3，存在$f(x)$在$F$上的分裂域$E$. 取$p_i(x)$的一个根$\alpha_i$，$i=1,2,\cdots,m$. 显然$\alpha_i\in E$，从而$E\supset F(\alpha_1,\alpha_2,\cdots,\alpha_m)\supset F$. 由第十七章，一，2，注2)，$E$是$F$的有限扩域. 由第十六章，一，9，2)，$F(\alpha_1,\alpha_2,\cdots,\alpha_m)$是$F$的有限扩域，且$\alpha_i$在$F$上极小多项式是$p_i(x)$.

4. 令P是一个特征为素数p的域，$F=P(\alpha)$是P的一个单扩域，而α是$P[x]$的多项式x^p-a的一个根. $P(\alpha)$是不是x^p-a在P上的分裂域？

解 已知$F=P(\alpha)$. 因$\alpha(\in F)$是$x^p-a(\in P[x])$的一个根，故$\alpha^p-a=0$，即$a=\alpha^p$. 由第十一章，三，9，1)，3)，$\mathrm{ch}\,P=\mathrm{ch}\,F=\mathrm{ch}\,F[x]=$素数$p$，从而由第十章，三，4，1)，在$F[x]$中，$x^p-a=x^p-\alpha^p=(x-\alpha)^p$. 于是$\alpha$是$x^p-a$的$p$重根，因此$P(\alpha)$就是添加$x^p-a$的$p$个相同的根$\alpha$于$P$而得到的扩域，所以$P(\alpha)$是$x^p-a$在$P$上的分裂域.

注 1) 第十七章，二，2中，α是x^3-a的根，而$\mathbb{Q}(\alpha)$不是x^3-a在$\mathbb{Q}$上的分裂域. 在本题中，α是x^p-a的根，$P(\alpha)$却是x^p-a在P上的分裂域. 关键区别在于$\mathrm{ch}\,\mathbb{Q}=\infty$，$\mathrm{ch}\,P=$素数$p$.

2) 设P是特征为素数p的域，因为1是$x^p-1(\in P[x])$的根，所以由该题知，$P(1)=P$是x^p-1在P上的分裂域.

5. 令F是一个含p^n个元的有限域. 证明：对于n的每一个因数$m>0$，存在并且只存在F的一个有p^m个元的子域L.

证 因$m\mid n$，故$n=mq$，q是正整数. 从而

$$\begin{aligned}p^n-1&=p^{mq}-1=(p^m)^q-1=(p^m-1)[(p^m)^{q-1}+(p^m)^{q-2}+\cdots+p^m+1]\\&=(p^m-1)k,\end{aligned}$$

其中$k=(p^m)^{q-1}+(p^m)^{q-2}+\cdots+p^m+1$. 于是

$$x^{p^n-1}-1=x^{(p^m-1)k}-1=(x^{p^m-1}-1)[(x^{p^m-1})^{k-1}+\cdots+1],$$

即$x^{p^m-1}-1\mid x^{p^n-1}-1$，从而$x^{p^m}-x\mid x^{p^n}-x$，所以$x^{p^m}-x$的根都是$x^{p^n}-x$的根.

因 F 是含 p^n 个元的有限域，故由第十七章，一，6，F 是 $x^{p^n}-x$ 在 F 的素子域上的分裂域. 由第十七章，一，7，$F=\{x^{p^n}-x$ 的 p^n 个根$\}$. 作 $L=\{x^{p^m}-x$ 的 p^m 个根$\}$. 因 $x^{p^m}-x$ 的根都是 $x^{p^n}-x$ 的根，故 $L\subset F$. 由第十七章，一，7 中命题的证明，L 是含 p^m 个元的 F 的子域. 实际上 L 是 $x^{p^m}-x$ 在 L 的素子域即 F 的素子域上的分裂域. 存在性证毕.

若 L_1 也是含 p^m 个元的 F 的子域，则依第十七章，一，6，L_1 是 $x^{p^m}-x$ 在 L_1 的素子域即 F 的素子域上的分裂域，因此 L_1 也是由 $x^{p^m}-x$ 在 F 中的所有根作成的，所以 $L_1=L$. 唯一性证毕.

注　1)　该命题的逆命题也成立. 即：设 F 是含 p^n 个元的有限域，若 L 是 F 的子域，则 L 是含 p^m 个元的有限域，且 $m\mid n$.

事实上，因 F 是有限域，故 F 的子域 L 也是有限域. 因 F 含 p^n 个元，故 $\mathrm{ch}\,F=p$，$(F:\Delta)=n$，其中 Δ 是 F 的素子域. 由第十一章，三，9，1)，$\mathrm{ch}\,L=p$. 由第十七章，一，7，L 含 p^m 个元，且 $m=(L:\Delta')$，其中 Δ'是 L 的素子域. 因 L 是 F 的子域，故 $\Delta'=\Delta$. 从而由第十六章，一，9，2)及第十六章，一，9，$n=(F:\Delta)=(F:L)(L:\Delta)=(F:L)m$，于是 $m\mid n$.

另一证法，由前一证法，已知 L 是含 p^m 个元的有限域，下面证明 $m\mid n$. L 的乘群 L^* 含 p^m-1 个元 . F 的乘群 F^* 含 p^n-1 个元. 因 $L^*\subset F^*$，故 L^* 是 F^* 的子群，从而由 Legrange 定理，$p^m-1\mid p^n-1$. 又 $p^n-1=(p^m-1)(p^{n-m}+p^{n-2m}+\cdots+p^{n-km})+p^{n-km}-1$，因此必存在正整数 k，使 $p^{n-km}-1=0$，即 $p^{n-km}=1$. 于是 $n=km$，所以 $m\mid n$.

2)　由该命题及注 1)知，含 p^n 个元的有限域的子域的个数恰为 n 的正因子的个数.

例　因 4 的正因子共 3 个：1，2，4，故含 $3^4=81$ 个元的有限域的子域恰有 3 个：分别为含 3，$3^2=9$，$3^4=81$ 个元的有限域.

6. 证明：一个有限域一定有比它大的代数扩域.

证一　设 F 是有限域，则由第十七章，一，6，F 是 $x^{p^m}-x$ 在 Δ 上的分裂域，其中 Δ 是特征为 p 的 F 的素子域. 取正整数 n，使 $n\neq m$，$m\mid n$. 由第十七章，一，3，有 $x^{p^n}-x(\in\Delta[x])$在 Δ 上的分裂域 E，则 $E\neq F$，且由上面 5 题知 E 是 F 的扩域. 因 Δ 是 E 的素子域，F 是 E 的子域，故由第十六章，四，1，1)，$\Delta\subset F$. 因 $x^{p^n}-x$ 的根都是 Δ 上的代数元，故 $x^{p^n}-x$ 的根都是 F 上的代数元. 所以 E 是 F 的真代数扩域.

（在证明了 E 是 F 的扩域，$E\neq F$ 以后，还可如下证明 E 是 F 的代数扩域：因 E 是 $x^{p^n}-x$ 在 Δ 上的分裂域，故 E 是 Δ 的代数扩域. 又 $E\supset F\supset\Delta$，从而由第十六章，二，6，注 3)，E 是 F 的代数扩域.）

证二　设 F 是含 q 个元的有限域，则由第十七章，一，6，F 是 x^q-x 在 Δ 上的分裂域，其中 Δ 是 F 的素子域. 考察 F 上多项式 $f(x)=x^q-x+1$. 因 $F[x]$是唯一分解环，$f(x)\neq 0$，$f(x)\neq$ 单位，故 $f(x)$在 F 上有不可约因子 $p(x)$. 于是 $p(x)$的任一根 $\beta\overline{\in}F$. 这是因为，$p(x)\mid f(x)$，β 是 $p(x)$的根，从而 β 是 $f(x)=x^q-x+1$ 的根，即 $f(\beta)=\beta^q-\beta+1=0$，$\beta^q-\beta=-1\neq 0$，$\beta$ 不是 x^q-x 的根，因此 $\beta\overline{\in}F$.

由第十七章，一，3，存在 $p(x)$在 F 上的分裂域 E. 于是由第十七章，一，2，注 2)，E 是 F 的代数扩域. 设 α 是 $p(x)$的一个根，则$\alpha\in E$但 $\alpha\overline{\in}F$，从而 $E\neq F$. 所以 E 是 F 的真代数扩域.

（在证明了 $p(x)$的任一根都$\overline{\in}F$ 以后，还可如下继续证明：设 α 是 $p(x)$的一个根，则

$\alpha \overline{\in} F$,即 $F(\alpha) \neq F$.从而 $F(\alpha)$是 F 的真代数扩域.)

注 1) 在证一中,取 $n=2m$,则 $x^{p^{2m}}-x$ 在 Δ 上的分裂域 E 就是 F 的真代数扩域.当然取 $n=km$,k 是任意大于 1 的整数,都是可以的.因此有限域有无穷多个真代数扩域.

2) 因为有限域有真代数扩域,所以有限域不是代数闭域.

3) 设 F 是 $x^{p^m}-x$ 在 Δ 上的分裂域,E 是 $x^{p^n}-x$ 在 Δ 上的分裂域,其中 $n>m$,Δ 是 F(也是 E)的素子域,则 E 未必是比 F 大的代数扩域.

例 $x^{2^2}-x$ 在 $\mathbb{Z}_2$上的分裂域是 $F=\{0,1,\omega,\omega^2\}$,其中 $\omega=-\dfrac{1}{2}+\dfrac{\sqrt{3}}{2}\mathrm{i}$. $x^{2^3}-x$ 在 $\mathbb{Z}_2$上的分裂域设为 E.因 $\omega^{2^3}-\omega=\omega^8-\omega=\omega^2-\omega=-\sqrt{3}\mathrm{i}\neq 0$,故 ω 不是 $x^{2^3}-x$ 的根,所以 $\omega \overline{\in} E$,从而 E 不是 F 的扩域.

7. 令 F 是一个有限域,Δ 是它所含素域,且 $F=\Delta(\alpha)$. α 是否必须是 F 的非零元所作的乘群的一个生成元?

解 已知 $F=\Delta(\alpha)$.由第十七章,一,9 中命题的证明,有限域 F 的乘群 F^* 是一个循环群,但 α 未必是 F^* 的生成元.

例 1 $\mathbb{Z}_3=\{0,1,2\}$是有限域,$\mathbb{Z}_3$的素子域是自身,则 $\mathbb{Z}_3=\mathbb{Z}_3(1)$. $\mathbb{Z}_3$的乘群 $\mathbb{Z}_3^*=\{1,2\}$.但 1 生成的循环群$(1)=\{1\}\neq \mathbb{Z}_3^*$,故 1 不是 $\mathbb{Z}_3^*$ 的生成元.

例 2 $\mathbb{Z}_3=\{0,1,2\}$是特征为 3 的素域.因 $p(x)=x^2+1(\in \mathbb{Z}_3[x])$在 $\mathbb{Z}_3$中无根,故 $p(x)$在 $\mathbb{Z}_3$ 上不可约.由第十六章,二,4,存在 $F=\mathbb{Z}_3(\alpha)$,其中 α 在 $\mathbb{Z}_3$上极小多项式是 $p(x)=x^2+1$.因 $\mathrm{ch}\, F=\mathrm{ch}\, \mathbb{Z}_3=3$,$(F:\mathbb{Z}_3)=(\mathbb{Z}_3(\alpha):\mathbb{Z}_3)=2$,故 $F=\mathbb{Z}_3(\alpha)$恰含 $3^2=9$ 个元($F=\mathbb{Z}_3(\alpha)$即为 $x^{3^2}-x$ 在 $\mathbb{Z}_3$上的分裂域).从而 F 的乘群 F^* 的阶为 8.但 $\alpha^2=-1$,于是 $\alpha^4=1$.因此$|\alpha|\neq|F^*|$,所以 α 不是 F^* 的生成元.

例 3 $\mathbb{Z}_2=\{0,1\}$是特征为 2 的素域.因 $p(x)=x^4+x^3+x^2+x+1$ 在 $\mathbb{Z}_2$中无根,故 $p(x)$在 $\mathbb{Z}_2$上无一次和三次因子.又 $p(x)$在 $\mathbb{Z}_2$上不能分解为两个二次因子的积.事实上,假定

$$\begin{aligned} p(x) &= x^4+x^3+x^2+x+1=(x^2+ax+b)(x^2+cx+d) \\ &= x^4+(a+c)x^3+(b+d+ac)x^2+(ad+bc)x+bd, \end{aligned}$$

其中 $a,b,c,d\in \mathbb{Z}_2$.因 $bd=1$,故 $b\neq 0,d\neq 0$,从而 $b=d=1$.因 $a+c=1$,故 a,c 中一个是 1,另一个是 0,即 $ac=0$,代入 $b+d+ac=1$ 中,得 $1+1+0=1$,即 $0=1$,矛盾.所以 $p(x)$在 $\mathbb{Z}_2$上不可约.存在 $F=\mathbb{Z}_2(\alpha)$,其中 α 在 $\mathbb{Z}_2$上极小多项式是 $p(x)$.因 $\mathrm{ch}\, F=2$,$(F:\mathbb{Z}_2)=4$,故 $F=\mathbb{Z}_2(\alpha)$恰含 $2^4=16$ 个元.于是 F 的乘群 F^* 的阶为 15.因 $\alpha^5-1=(\alpha-1)(\alpha^4+\alpha^3+\alpha^2+\alpha+1)=(\alpha-1)0=0$,故 $\alpha^5=1$,从而 α 的阶$|\alpha|\neq|F^*|$,所以 α 不是 F^* 的生成元.

注 例 2 中,$F=\mathbb{Z}_3(\alpha)=\{a+b\alpha \mid a,b\in \mathbb{Z}_3\}=\{0,1,2,\alpha,1+\alpha,2+\alpha,2\alpha,1+2\alpha,2+2\alpha\}$. $|F^*|=8$,而$|1+\alpha|=|2+\alpha|=|1+2\alpha|=|2+2\alpha|=8$,故 $F^*=(1+\alpha)=(2+\alpha)=(1+2\alpha)=(2+2\alpha)$.由第十七章,一,9,$F=\mathbb{Z}_3(\alpha)=\mathbb{Z}_3(1+\alpha)=\mathbb{Z}_3(2+\alpha)=\mathbb{Z}_3(1+2\alpha)=\mathbb{Z}_3(2+2\alpha)$.

8. 令 Δ 是特征为 2 的素域.找出 $\Delta[x]$的一切三次不可约多项式.

解 因 Δ 是特征为 2 的素域,故由第十六章,一,1,注 1),Δ 恰含 2 个元,从而 $\Delta=\{0,1\}$.设 $\Delta[x]$的任意一个三次不可约多项式为 $f(x)=a_3x^3+a_2x^2+a_1x+a_0$,其中 $a_i\in\Delta$.因 $\deg f(x)=3$,故 $a_3\neq 0$,从而 $a_3=1$.因 $f(x)$在 Δ 上不可约,故 $a_0\neq 0$,从而 $a_0=1$.

1) 若 $a_2=a_1=1$.因 1 是 x^3+x^2+x+1 的根,故由第十五章,三,3,x^3+x^2+x+1 在

Δ 上可约.

2) 若 $a_2=a_1=0$. 因 1 是 x^3+1 的根,故同上理,x^3+1 在 Δ 上可约.

3) 若 $a_2=1,a_1=0$. 因 x^3+x^2+1 在 Δ 中无根,故由第十五章,三,3,注,x^3+x^2+1 在 Δ 上不可约.

4) 若 $a_2=0,a_1=1$,则同上理,x^3+x+1 在 Δ 上不可约.

所以 $\Delta(x)$ 的一切三次不可约多项式是 x^3+x^2+1 与 x^3+x+1.

9. 令域 F 的特征是 p, $f(x)$ 是 F 上一个不可约多项式,并且 $f(x)$ 可以写成 F 上 x^{p^e},但不能写成 $x^{p^{e+1}}$ 的多项式($e\geqslant 1$). 证明:$f(x)$ 的每一个根的重复度都是 p^e.

证 首先给出定义:设 I 是整环,$\alpha\in I$, $f(x)\in I[x]$,则

$$\alpha \text{ 是 } f(x) \text{ 的 } k \text{ 重根}(k \text{ 是 } \alpha \text{ 的重数或重复度})$$

$$\Leftrightarrow (x-\alpha)^k \mid f(x),\ (x-\alpha)^{k+1} \nmid f(x).$$

因 $f(x)$ 可以写成 F 上 x^{p^e} 的多项式,故可设 $f(x)=g(x^{p^e})=g(y)$,其中 $y=x^{p^e}$. 因 $f(x)$ 在 F 上不可约,故 $g(y)$ 在 F 上不可约. 由第十七章,一,3,存在 $g(y)$ 在 F 上的分裂域 E,使

$$g(y)=a_m(y-\beta_1)(y-\beta_2)\cdots(y-\beta_m),$$

其中 $a_m\in F,\beta_i\in E,i=1,2,\cdots,m$. 从而

$$f(x)=a_m(x^{p^e}-\beta_1)(x^{p^e}-\beta_2)\cdots(x^{p^e}-\beta_m).$$

设 α_i 是 $x^{p^e}-\beta_i$ 的一个根,则 $\alpha_i^{p^e}=\beta_i$. 因 $\mathrm{ch}\ F=\mathrm{ch}\ E=\mathrm{ch}\ E[x]=$ 素数 p,故由第十章,三,4,2),

$$x^{p^e}-\beta_i=x^{p^e}-\alpha_i^{p^e}=(x-\alpha_i)^{p^e}.$$

因此

$$f(x)=a_m(x-\alpha_1)^{p^e}(x-\alpha_2)^{p^e}\cdots(x-\alpha_m)^{p^e}.$$

下面只需证明 $\alpha_1,\alpha_2,\cdots,\alpha_m$ 互不相同. 假设 $\alpha_i=\alpha_j(i\neq j)$,则 $x^{p^e}-\beta_i$ 与 $x^{p^e}-\beta_j$ 有公共根 $\alpha_i=\alpha_j$,即 $\alpha_j^{p^e}-\beta_i=\alpha_j^{p^e}-\beta_j=0$. 于是 $g(y)$ 有重根 $\beta_i=\beta_j(i\neq j)$. 因 $g(y)$ 在 F 上不可约,$\mathrm{ch}\ F=p$. 故由第十七章,一,11,$g(y)=h(y^p)$,这里 $h(y)$ 是 F 上的一个多项式,从而

$$f(x)=g(x^{p^e})=g(y)=h(y^p)=h((x^{p^e})^p)=h(x^{p^{e+1}}),$$

此与已知 $f(x)$ 不能写成 $x^{p^{e+1}}$ 的多项式矛盾. 所以 $\alpha_1,\alpha_2,\cdots,\alpha_m$ 互不相同. 即 $f(x)$ 有 m 个互不相同的根 $\alpha_1,\alpha_2,\cdots,\alpha_m$,且它们的重复度都是 p^e.

注 设 $\deg f(x)=n$, $f(x)$ 有 m 个不同的根,它们的重复度都是 p^e,则 $n=mp^e$.

10. 设域 F 没有不可离扩域. 证明:F 的任一代数扩域都没有不可离扩域.

证一 若 E 是 F 的代数扩域. 假设 E 有不可离扩域 K,则由定义,K 中有元 α 不是 E 上可离元,从而 α 在 E 上极小多项式 $p(x)$ 有重根. 因 K 是 E 的代数扩域,E 是 F 的代数扩域,故由第十六章,一,6,注 3),K 是 F 的代数扩域. 由已知条件,K 是 F 的可离扩域,从而 $\alpha(\in K)$ 是 F 上可离元,于是 α 在 F 上极小多项式 $g(x)$ 没有重根. 由第十六章,一,6,注 7),在 $E[x]$ 中,$p(x)\mid g(x)$. 因 $g(x)$ 没有重根,故 $p(x)$ 没有重根,此与 $p(x)$ 有重根矛盾. 所以命题得证.

证二 设 E 是 F 的任一代数扩域. 只需证明 E 上任一代数元 α 都是 E 上可离元,只需证明 α 在 E 上极小多项式 $p(x)$ 没有重根. 事实上,因 α 是 E 上代数元,E 是 F 的代数扩域,

故由第十六章，二，6，α是F上代数元. 因F没有不可离扩域，故α是F上可离元，从而α在F上极小多项式$g(x)$没有重根. 由第十六章，一，6，注 7)，在$E[x]$中，$p(x)\mid g(x)$，于是$p(x)$也没有重根. 所以E上任一代数元都是E上可离元，因此F的任一代数扩域E都没有不可离扩域.

11. 令域F的特征是p而$E=F(\alpha,\beta)$，这里α是F上n次可离元而β是F上p次非可离元. $(E:F)=?$

解 因α,β是F上代数元，故$E=F(\alpha,\beta)$是F的有限扩域，从而由第十六章，一，9，

$$(E:F)=(F(\alpha,\beta):F)=(F(\alpha)(\beta):F(\alpha))(F(\alpha):F).$$

已知$(F(\alpha):F)=n$，今要求出$(E:F)$，只需求出$(F(\alpha)(\beta):F(\alpha))$.

因β是F上p次代数元，故β在F上极小多项式$f(x)$是p次的. 设β在$F(\alpha)$上极小多项式是$h(x)$，由第十六章，一，6，注 7)，在$F(\alpha)$中，$h(x)\mid f(x)$，从而$0<\deg h(x)\leqslant\deg f(x)=p$. 假定$\deg h(x)<p$，则$h(x)\neq g(x^p)$，这里$g(x)$是$F(\alpha)$上的一个多项式. 因$h(x)$在$F(\alpha)$上不可约，$\mathrm{ch}\,F(\alpha)=\mathrm{ch}\,F=$素数$p$，故由第十七章，一，11，$h(x)$没有重根，于是$\beta$是$F(\alpha)$上可离元，而已知$\alpha$是$F$上可离元，由第十七章，一，14，$\beta$也是$F$上可离元，此与已知矛盾. 所以$\deg h(x)=p$. 即$(F(\alpha)(\beta):F(\alpha))=p$. 于是$(E:F)=pn$.

12. 找一个域F，使F有一个有限扩域E而E不是F的单扩域.

解 设Δ是特征为素数p的素域. 取$F=\Delta(x^p,y^p)$，其中x,y是Δ上无关未定元. 于是x^p,y^p也是Δ上无关未定元. 否则，若x^p,y^p不是Δ上无关未定元，则$\exists$不全为0的元，$a,b\in\Delta$，使得$ax^p+by^p=0$，于是x,y不是Δ上无关未定元，矛盾. 与第十七章，一，12，注 2)，(ii)同理可知：x在$F=\Delta(x^p,y^p)$上极小多项式为z^p-x^p，而y在$F=\Delta(x^p,y^p)$上极小多项式为z^p-y^p，从而y在$F(x)=\Delta(x^p,y^p)(x)$上极小多项式也为z^p-y^p. 于是

$$(F(x):F)=p\quad,\quad(F(x,y):F(x))=p.$$

令$E=F(x,y)=\Delta(x^p,y^p)(x,y)$，则由第十六章，一，9，

$$(E:F)=(E:F(x))(F(x):F)=p^2.$$

所以E是F的有限扩域. 但E不是F的单扩域. 事实上，假设$E=F(\theta)$，则$\theta(\in E=F(x,y))$可以写成F上x,y的有理式：$\theta=\dfrac{f(x,y)}{g(x,y)}$，其中$f(x,y),g(x,y)(\neq 0)$的系数都$\in F$. 于是$\theta^p=\dfrac{(f(x,y))^p}{(g(x,y))^p}$. 因$\mathrm{ch}\,F[x,y]=\mathrm{ch}\,F=\mathrm{ch}\,\Delta=$素数$p$，故由第十章，三，4，3)，$(f(x,y))^p$，$(g(x,y))^p$是$f(x,y),g(x,y)$的各项的$p$次方的和，从而$\theta^p$是在$F=\Delta(x^p,y^p)$上$x^p,y^p$的有理式，因此$\theta^p\in F$. 由第十六章，二，2，注 1)，$\theta^p$在$F$上极小多项式是一次的：$z-\theta^p$. 从而$\theta$在$F$上极小多项式可能是$p$次的：$z^p-\theta^p$，也可能是低于$p$次的(因$z^p-\theta^p$可能在$F$上可约). 总之，$(E:F)=(F(\theta):F)\leqslant p$. 又已知$(E:F)=p^2$，于是$p^2\leqslant p$，这里$p$是素数，矛盾. 所以$E$是$F$的有限扩域而不是$F$的单扩域.

注 1) 若取$F=\Delta(x,y)$，x,y是Δ上无关未定元，令α,β分别是z^p-x,z^p-y的根，即$\alpha^p=x,\beta^p=y$，记$\alpha=x^{\frac{1}{p}},\beta=y^{\frac{1}{p}}$. 此时同理知$E=F(x^{\frac{1}{p}},y^{\frac{1}{p}})$是$F$的有限扩域而不是$F$的单扩域. 因为这里与前者只是符号上的差别.

2) 由本题知，若将第十七章，一，17 中“可离”这一条件去掉，结论不成立.

三、讲与练

1. 试判断下面各命题是否正确.

1)　实数域$\mathbb{R}$是代数闭域.

2)　设E是代数闭域,F是E的子域,则E是任一$n(>0)$次多项式$(\in F[x])$在F上的分裂域.

3)　设E是$f(x)$在域F上的分裂域,则E是代数闭域.

4)　设$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$是$f(x)$在域$F$上的分裂域,则$\alpha_1,\alpha_2,\cdots,\alpha_n$是$f(x)$的全部根.

5)　设E是$f(x)$在域F上的分裂域,K是E的子域且$E\supset K\supset F$,则E也是$f(x)$在K上的分裂域.

6)　设F是域,则任何一次多项式$f(x)(\in F[x])$在F上的分裂域是F本身.

7)　设P是特征为素数p的域,则x^p-1在P上的分裂域是P自身.

8)　特征为素数p的域F必为有限域.

9)　F是特征为素数p的素域$\Leftrightarrow F$是含素数p个元的有限域.

10)　设域F的特征为素数p,F中任一元都是x^p-x的根,则F是素域.

11)　若有限域F含偶数个元,则F恰含2^n个元,其中$n=(F:\Delta)$,Δ是F的素子域.

12)　设Δ是特征为素数p的素域,则对于任意一个正整数n,必在Δ上存在n次不可约多项式.

13)　设$GF(p^m)$,$GF(p^n)$是域E的两个有限子域,$\mathrm{ch}\,E=$素数p,则$GF(p^m)\subset GF(p^n)\Leftrightarrow m\mid n$.

14)　设p,q为素数,则含p^q个元的域F中除素子域外,没有其他的真子域.

15)　设E是有p^n个元的有限域,$\mathrm{ch}\,E=p$,$n=(E:\Delta)$,Δ是E的素子域,则$\forall\alpha\in E$,E上多项式$x^p-\alpha$在E里有根.

16)　设E是域F的可离扩域,I是E的子域,且$F\subset I\subset E$,则E也是I的可离扩域.

解　1)　不正确.因为$\mathbb{R}$有真代数扩域:复数域$\mathbb{C}$.

2)　不正确.例,$\mathbb{C}$是代数闭域,$\mathbb{Q}$是$\mathbb{C}$的子域,但$\mathbb{C}$不是x^2+1在$\mathbb{Q}$上的分裂域$\mathbb{Q}(\mathrm{i})$.

3)　不正确.例,$x^3-5x^2+9x-9=(x-3)(x^2-2x+3)=(x-3)[x-(1+\sqrt{2}\mathrm{i})][x-(1-\sqrt{2}\mathrm{i})]$在$\mathbb{Q}$上的分裂域是$\mathbb{Q}(3,1+\sqrt{2}\mathrm{i},1-\sqrt{2}\mathrm{i})=\mathbb{Q}(\sqrt{2}\mathrm{i})$. $\mathbb{Q}(\sqrt{2}\mathrm{i})$,有真代数扩域$\mathbb{C}$.所以$\mathbb{Q}(\sqrt{2}\mathrm{i})$不是代数闭域.

4)　不正确.例,x^3-x的全部根是$0,1,2\in\mathbb{Z}_3$,从而x^3-x在域$\mathbb{Z}_3$上的分裂域是$\mathbb{Z}_3(0,1,2)=\mathbb{Z}_3$.当然有$\mathbb{Z}_3=\mathbb{Z}_3(0)$,但0不是$x^3-x$的全部根.

5)　正确.事实上,设$f(x)$的根是$\alpha_1,\alpha_2,\cdots,\alpha_n$,则由第十七章,一,2,$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$,且$f(x)$在$K$上的分裂域$E'=K(\alpha_1,\alpha_2,\cdots,\alpha_n)$,显然$E\subset E'$;反之,因$K\subset E$,$\alpha_1,\alpha_2,\cdots,\alpha_n\in E$,故$K(\alpha_1,\alpha_2,\cdots,\alpha_n)=E'\subset E$.所以$E=E'$.

6)　正确.事实上,设$f(x)=ax+b=a\left[x-\left(-\dfrac{b}{a}\right)\right]$,则$f(x)$的根$-\dfrac{b}{a}\in F$,从而$f(x)$

在 F 上的分裂域是 $F\left(-\frac{b}{a}\right)=F$.

7) 正确.事实上,因 1 是 $P[x]$的多项式 x^p-1 的一个根,又 ch $P=p$,故由第十七章,二,4,注 2),$P(1)=P$ 是 x^p-1 在 P 上的一个分裂域.

8) 不正确.例,设 F 是特征为素数 p 的有限域,x 是 F 上未定元,$F(x)$是 F 上一元多项式环 $F(x)$的商域,由第十三章,三,5,1)及第十章,三,9,3)知,ch $F(x)=$ ch $F[x]=$ ch $F=p$.因 $F[x]\subset F(x)$,而 $F[x]$里有任意高次的多项式,所以 $F[x]$中也就是 $F(x)$中有无限多个元,于是 $F(x)$不是有限域.

注 ① 由第十六章,一,1,注 4),若 E 是有限域,则 E 的特征为素数.上例说明该命题的逆命题不成立.若 E 是特征为素数 p 的有限域,则 E 含 p^n 个元,n 是正整数.

② 设 F 是特征为素数 p 的有限域,x 是 F 上未定元.把域 $F(x)$看成加群,则 $F(x)$是一个无限加群,而 $F(x)$中的非零元的阶都是 p,零元 0 的阶是 1,从而 $F(x)$的每个元的阶都有限.

同样,环 $F[x]$也是一个无限加群,但其中每个元的阶都有限.

说明第四章,二,6 的逆命题不成立.

9) 正确.事实上,($\Rightarrow$) $F\cong\mathbb{Z}_p$,$\mathbb{Z}_p$含 p 个元,从而 F 也是含 p 个元的有限域.($\Leftarrow$) ch $F=p$.设 Δ 是 F 的素子域,则因 F 含 p^1 个元,故$(F:\Delta)=1$.由第十六章,一,12,$F=\Delta$ 是一个素域.

10) 正确.事实上,由上题 9),只需证明 F 含 p 个元.因 F 中任一元都是 x^p-x 的根,故 F 最多有 p 个元;设 Δ 是 F 的素子域,因 ch $\Delta=$ ch $F=p$,故由上题 9)($\Rightarrow$),$\Delta(\subset F)$含 p 个元,于是 F 最少有 p 个元.所以 F 含 p 个元.由上题 9),F 是素域.

11) 正确.事实上,因 F 必含 p^n 个元,其中 p 是素数,今 $p^n=2k$,k 是正整数,故 $2\mid p^n$,但 p 是素数,从而 $p=2$,于是 F 含 2^n 个元,其中 $n=(F:\Delta)$,Δ 是 F 的素子域.

12) 正确.事实上,对于每个正整数 n,$x^{p^n}-x$ 在 Δ 上的分裂域 E 是一个含 p^n 个元的有限域,因此$(E:\Delta)=n$.由第十七章,一,9,E 是 Δ 的单扩域,设 $E=\Delta(\alpha)$,即$(\Delta(\alpha):\Delta)=n$.所以存在 α 在 Δ 上极小多项式 $p(x)$,$p(x)$就是一个 Δ 上 n 次不可约多项式.

13) 正确.由第十七章,二,5 及其注 1)可知.

14) 正确.事实上,设 L 是 F 的子域,则由第十七章,二,5,注 1),L 是含 p^m 个元的有限域,且 $m\mid q$.因 q 是素数,故只能 $m=1$ 或 q.从而 L 只能是 F 的素子域或 F 自身.所以命题得证.

15) 正确.事实上,由第十七章,一,7,注 3),$E=\{x^{p^n}-x$ 的全部根$\}$.$\forall\alpha\in E$,α 是 $x^{p^n}-x$ 的根,即 $\alpha^{p^n}-\alpha=0$,从而$(\alpha^{p^{n-1}})^p-\alpha=0$,因此 $\alpha^{p^{n-1}}(\in E)$是 $x^p-\alpha$ 的根.

16) 正确.事实上,$\forall\alpha\in E$,因 E 是 F 的可离扩域,故 α 是 F 上可离元.今 I 是 F 的扩域,由第十七章,一,13,注 1),α 也是 I 上可离元.所以 E 也是 I 的可离扩域.

2. 设 F 是域,$f(x)=x^2+ax+b\in F[x]$.证明:若 $f(x)$在 F 上可约,则 F 是$f(x)$在 F 上的分裂域;若 $f(x)$在 F 上不可约,则 $f(x)$在 F 上的分裂域是 F 的单代数扩域.

证 若 $f(x)$在 F 上可约,则 $f(x)=(x-\alpha)(x-\beta)$,其中 $\alpha,\beta\in F$,从而 $f(x)$在 F 上的分裂域是 $F(\alpha,\beta)=F$.

若 $f(x)$ 在 F 上不可约，由第十六章，二，4，存在 F 的单代数扩域 $F(\alpha)$. 其中 α 在 F 上极小多项式是 $f(x)$，从而 $f(x)=(x-\alpha)g(x)\in F(\alpha)[x]$. 由第十一章，四，1，10)，$g(x)$ 是一次的，于是 $g(x)=x-\beta$，其中 $\beta\in F(\alpha)$. 所以 $f(x)$ 在 F 上的分裂域是 $F(\alpha,\beta)=F(\alpha)$.

例 1　因 $f(x)=x^2-x-2=(x-2)(x+1)$ 在 $\mathbb{Q}$ 上可约，故 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域是 $\mathbb{Q}$.

例 2　因 $f(x)=x^2+2=(x-\sqrt{2}\,\mathrm{i})(x+\sqrt{2}\,\mathrm{i})$ 在 $\mathbb{Q}$ 上不可约，故 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域是 $\mathbb{Q}(\sqrt{2}\,\mathrm{i})$.

例 3　因 $f(x)=x^2+x+1$ 在 $\mathbb{Z}_2$ 上不可约，设 α 是 $f(x)$ 的一个根，故 $f(x)$ 在 $\mathbb{Z}_2$ 上的分裂域是 $\mathbb{Z}_2(\alpha)$.

3. 试求出下面各多项式 $f(x)$ 在域 F 上的分裂域 E，并确定 $(E:F)$.

1)　$f(x)=x^p-1$，p 是素数. $F=\mathbb{Q}$.

2)　$f(x)=x^4-1$. $F=\mathbb{Q}$.

3)　$f(x)=x^{p^n}-1$，其中 p 是素数，n 是正整数，$\mathrm{ch}\,F=p$.

4)　$f(x)=x^4-3$. $F=\mathbb{Q}$.

5)　$f(x)=x^5-2$. $F=\mathbb{Q}$.

6)　$f(x)=x^3-x^2-x-2$. $F=\mathbb{Q}$.

7)　$f(x)=x^4-x^2-2$. $F=\mathbb{Q}$.

8)　$f(x)=x^4+x^3+x^2+1$. $F=\mathbb{Z}_2$. $\mathbb{Z}_2$ 中元 $[a]$ 表为 a.

解　1)　$f(x)=x^p-1=(x-1)(x^{p-1}+x^{p-2}+\cdots+1)$. 由第十五章，四，14，$g(x)=x^{p-1}+x^{p-2}+\cdots+1$ 在 $\mathbb{Q}$ 上不可约. 由第十六章，三，2，7)，p 次本原单位根 $\alpha=\cos\dfrac{2\pi}{p}+\mathrm{i}\sin\dfrac{2\pi}{p}$ 是 $g(x)$ 的一个根. $\alpha^0=1,\alpha,\alpha^2,\cdots,\alpha^{p-1}$ 是 $f(x)$ 的 p 个不同的根. 从而 $E=\mathbb{Q}(1,\alpha,\alpha^2,\cdots,\alpha^{p-1})=\mathbb{Q}(\alpha)$. $(\mathbb{Q}(\alpha):\mathbb{Q})=p-1$.

注　$x^{p-1}+x^{p-2}+\cdots+1$ 与 x^p-1 在 $\mathbb{Q}$ 上的分裂域相同，其中 p 是素数.

例 1　x^5-1 在 $\mathbb{Q}$ 上的分裂域是 $\mathbb{Q}(\alpha)$，这里 $\alpha=\cos\dfrac{2\pi}{5}+\mathrm{i}\sin\dfrac{2\pi}{5}$. $(\mathbb{Q}(\alpha):\mathbb{Q})=4$.

例 2　$x^{17}-1$ 在 $\mathbb{Q}$ 上的分裂域是 $\mathbb{Q}(\alpha)$，这里 $\alpha=\cos\dfrac{2\pi}{17}+\mathrm{i}\sin\dfrac{2\pi}{17}$. $(\mathbb{Q}(\alpha):\mathbb{Q})=16$.

2)　$f(x)=x^4-1=(x-1)(x^3+x^2+x+1)=(x-1)(x+1)(x^2+1)=(x-1)(x+1)\cdot(x-\mathrm{i})(x+\mathrm{i})$. $E=\mathbb{Q}(1,-1,\mathrm{i},-\mathrm{i})=\mathbb{Q}(\mathrm{i})$，$\mathrm{i}$ 是 4 次本原单位根. $(\mathbb{Q}(\mathrm{i}):\mathbb{Q})=2$.

注　因 x^4-1 的次数 4 不是素数，故 $(E:\mathbb{Q})\neq 4-1=3$. 又如 $x^{12}-1$ 在 $\mathbb{Q}$ 上的分裂域是 $\mathbb{Q}(\alpha)$，这里 $\alpha=\cos\dfrac{2\pi}{12}+\mathrm{i}\sin\dfrac{2\pi}{12}$. $(\mathbb{Q}(\alpha):\mathbb{Q})=4$，这是因为 α 在 $\mathbb{Q}$ 上极小多项式是 $x^4-x^2+1=(x-\alpha)(x-\alpha^5)(x-\alpha^7)(x-\alpha^{11})$（见第十六章，三，2，8)）.

一般来说，$x^n-1=(x-1)(x^{n-1}+x^{n-2}+\cdots+1)$ 在 $\mathbb{Q}$ 上的分裂域是 $\mathbb{Q}(\alpha)$，这里 $\alpha=\cos\dfrac{2\pi}{n}+\mathrm{i}\sin\dfrac{2\pi}{n}$.

3)　因 $\mathrm{ch}\,F[x]=\mathrm{ch}\,F=p$，故由第十章，三，4，2)，$x^{p^n}-1=x^{p^n}-1^{p^n}=(x-1)^{p^n}$，从而 $x^{p^n}-1$ 在 F 上的分裂域是 $F(1)=F$. $(F:F)=1$.

特别地，x^p-1 在域 F 上的分裂域是 F，这里 $\mathrm{ch}\,F=$ 素数 p（见第十七章，二，4，注 2)）. 此结论与本题 1)不同，就因为域 F 不同.

4) x^4-3 的根是 4 个 3 的 4 次方根：$\sqrt[4]{3}, \mathrm{i}\sqrt[4]{3}, \mathrm{i}^2\sqrt[4]{3}=-\sqrt[4]{3}, \mathrm{i}^3\sqrt[4]{3}=-\mathrm{i}\sqrt[4]{3}$，其中 i 是一个 4 次本原单位根. $E=\mathbb{Q}(\sqrt[4]{3}, \mathrm{i}\sqrt[4]{3}, -\sqrt[4]{3}, -\mathrm{i}\sqrt[4]{3})=\mathbb{Q}(\sqrt[4]{3}, \mathrm{i})$. 因 x^2+1 的两个根 $\pm\mathrm{i}$ 不是实数，故 $\pm\mathrm{i}\notin\mathbb{Q}(\sqrt[4]{3})$，从而 x^2+1 在 $\mathbb{Q}(\sqrt[4]{3})$ 上不可约，于是 i 在 $\mathbb{Q}(\sqrt[4]{3})$ 上极小多项式是 x^2+1. 由第十五章，四，13，艾森斯坦因不可约性判别准则，x^4-3 在 $\mathbb{Q}$ 上不可约，于是 x^4-3 是 $\sqrt[4]{3}$ 在 $\mathbb{Q}$ 上极小多项式. 所以

$$(E:\mathbb{Q})=(\mathbb{Q}(\sqrt[4]{3})(\mathrm{i}):\mathbb{Q}(\sqrt[4]{3}))(\mathbb{Q}(\sqrt[4]{3}):\mathbb{Q})=2\cdot 4=8.$$

5) x^5-2 的 5 个根是 $\sqrt[5]{2}, \omega\sqrt[5]{2}, \cdots, \omega^4\sqrt[5]{2}$，其中 $\omega=\cos\frac{2\pi}{5}+\mathrm{i}\sin\frac{2\pi}{5}$ 是 5 次本原单位根. $E=\mathbb{Q}(\sqrt[5]{2}, \omega\sqrt[5]{2}, \cdots, \omega^4\sqrt[5]{2})=\mathbb{Q}(\sqrt[5]{2}, \omega)$. 由艾森斯坦因不可约性判别准则，$x^5-2$ 在 $\mathbb{Q}$ 上不可约，从而 $\sqrt[5]{2}$ 在 $\mathbb{Q}$ 上极小多项式是 x^5-2. $g(x)=x^4+x^3+x^2+x+1=(x-\omega)(x-\omega^2)\cdot(x-\omega^3)(x-\omega^4)$，$\omega^i\notin\mathbb{Q}(\sqrt[5]{2})$，$\omega^i\omega^j$ 与 $\omega^i+\omega^j$ 不能同时 $\in\mathbb{Q}(\sqrt[5]{2})$，$i, j=1,2,3,4$. 于是 $g(x)$ 在 $\mathbb{Q}(\sqrt[5]{2})$ 上无一次因子与二次因子. 因此 $g(x)$ 在 $\mathbb{Q}(\sqrt[5]{2})$ 上不可约，从而 ω 在 $\mathbb{Q}(\sqrt[5]{2})$ 上极小多项式是 $g(x)$. 所以

$$(E:\mathbb{Q})=(\mathbb{Q}(\sqrt[5]{2})(\omega):\mathbb{Q}(\sqrt[5]{2}))(\mathbb{Q}(\sqrt[5]{2}):\mathbb{Q})=4\cdot 5=20.$$

注 ① x^n-a 的 n 个根是 $\sqrt[n]{a}, \omega\sqrt[n]{a}, \cdots, \omega^{n-1}\sqrt[n]{a}$，其中 $\omega=\cos\frac{2\pi}{n}+\mathrm{i}\sin\frac{2\pi}{n}$ 是一个 n 次本原单位根. x^n-a 在 $\mathbb{Q}$ 上的分裂域是 $\mathbb{Q}(\sqrt[n]{a}, \omega\sqrt[n]{a}, \cdots, \omega^{n-1}\sqrt[n]{a})=\mathbb{Q}(\sqrt[n]{a}, \omega)$.

② 设域 F 的特征是素数 p，则 x^p-a 在 F 上的分裂域是 $F(\alpha)$，其中 α 是 x^p-a 的一个根（见第十七章，二，4）.

6) $x^3-x^2-x-2=(x-2)(x^2+x+1)=(x-2)(x-\omega)(x-\omega^2)$，其中 $\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}$，$\omega^2=-\frac{1}{2}-\frac{\sqrt{3}}{2}\mathrm{i}$. $E=\mathbb{Q}(2, \omega, \omega^2)=\mathbb{Q}(\omega)=\mathbb{Q}(\sqrt{3}\,\mathrm{i})$. $(E:\mathbb{Q})=2$.

7) $x^4-x^2-2=(x^2-2)(x^2+1)=(x-\sqrt{2})(x+\sqrt{2})(x-\mathrm{i})(x+\mathrm{i})$. $E=\mathbb{Q}(\sqrt{2}, \mathrm{i})$. $(E:\mathbb{Q})=(\mathbb{Q}(\mathrm{i})(\sqrt{2}):\mathbb{Q}(\mathrm{i}))(\mathbb{Q}(\mathrm{i}):\mathbb{Q})=2\cdot 2=4$.

8) 1 是 $f(x)$ 的根，即 $x-1\mid f(x)$. 用带余除法得 $f(x)=(x-1)(x^3+x+1)$. 因 $1\in\mathbb{Z}_2$，故 $f(x)$ 在 $\mathbb{Z}_2$ 上的分裂域就是 $g(x)=x^3+x+1$ 在 $\mathbb{Z}_2$ 上的分裂域. 下面求 $g(x)$ 在 $\mathbb{Z}_2$ 上的分裂域.

因 $g(x)$ 在 $\mathbb{Z}_2$ 中无根，故 $g(x)$ 在 $\mathbb{Z}_2$ 上不可约. 由第十六章，二，4，存在 $\mathbb{Z}_2$ 的单代数扩域 $\mathbb{Z}_2(\alpha)$，其中 α 在 $\mathbb{Z}_2$ 上极小多项式是 $g(x)$. 从而 $g(x)=(x-\alpha)(x^2+ax+b)\in\mathbb{Z}_2(\alpha)[x]$，即

$$x^3+x+1=x^3+(a-\alpha)x^2+(b-a\alpha)x-b\alpha.$$

比较系数，得 $a-\alpha=0, b-a\alpha=1, -b\alpha=1$. 解得，$a=\alpha, b=\alpha^2+1$，即 $g(x)=(x-\alpha)[x^2+\alpha x+(\alpha^2+1)]$. 下面确定 $h(x)=x^2+\alpha x+(\alpha^2+1)$ 在 $\mathbb{Z}_2(\alpha)$ 上是否可约.

因 $(\mathbb{Z}_2(\alpha):\mathbb{Z}_2)=3$，故由第十六章，一，5，

$$\begin{aligned}\mathbb{Z}_2(\alpha)&=\{a_0+a_1\alpha+a_2\alpha^2 \mid a_i\in\mathbb{Z}_2\}\\&=\{0,1,\alpha,\alpha^2,1+\alpha,1+\alpha^2,\alpha+\alpha^2,1+\alpha+\alpha^2\}.\end{aligned}$$

将 $\mathbb{Z}_2(\alpha)$ 中的 α^2 代入 $h(x)$，

$$h(\alpha^2)=\alpha^4+\alpha^3+\alpha^2+1=(\alpha^4+\alpha^2+\alpha)+(\alpha^3+\alpha+1)$$
$$=\alpha(\alpha^3+\alpha+1)+(\alpha^3+\alpha+1)=(\alpha+1)g(\alpha)=0.$$

即 α^2 是 $h(x)$的一个根，从而 $h(x)$在 $\mathbb{Z}_2(\alpha)$上可约．由第十七章，三，2，$h(x)$的根都$\in\mathbb{Z}_2(\alpha)$．所以 $g(x)$也就是 $f(x)$在 $\mathbb{Z}_2$上的分裂域是 $\mathbb{Z}_2(\alpha)$．$(\mathbb{Z}_2(\alpha):\mathbb{Z}_2)=3$．

4. 试分别构造含 4，9，25，27，32，125 个元的有限域．

解　设 Δ 是有限域 $GF(p^n)$的素子域，则由第十七章，一，6；第十七章，一，9；第十六章，一，4，$GF(p^n)=x^{p^n}-x$ 在 Δ 上的分裂域$=\Delta(\alpha)\cong\mathbb{Z}_p(\alpha)\cong\mathbb{Z}_p[x]/(p(x))$，其中 $p(x)$是 α 在 $\mathbb{Z}_p$上的 n 次极小多项式．所以对于给定的素数 p，正整数 n，只要能找到 $\mathbb{Z}_p$上任意一个最高系数为 1 的 n 次不可约多项式 $p(x)$，由第十六章，一，5，就可以构造出 $GF(p^n)$，

$$GF(p^n)=\left\{\sum_{i=0}^{n-1}a_i\alpha^i\,\middle|\,a_i\in\mathbb{Z}_p\right\},$$

其中 α 是 $p(x)$的一个根．由第十七章，三，1，12)知，对于任意素数 p 和正整数 n，必存在 $\mathbb{Z}_p$ 上 n 次不可约多项式．

1)　因 $4=2^2$，而 x^2+x+1 在 $\mathbb{Z}_2$上不可约(第十五章，三，4，6))，故

$$GF(4)=\mathbb{Z}_2(\alpha)=\{a_0+a_1\alpha\,|\,a_i\in\mathbb{Z}_2\}=\{0,1,\alpha,1+\alpha\},$$

其中 α 是 x^2+x+1 的一个根．

2)　因 $9=3^2$，而 x^2-x-1 在 $\mathbb{Z}_3$上不可约，故

$$GF(9)=\mathbb{Z}_3(\alpha)=\{a_0+a_1\alpha\,|\,a_i\in\mathbb{Z}_3\}$$
$$=\{0,1,2,\alpha,2\alpha,1+\alpha,1+2\alpha,2+\alpha,2+2\alpha\},$$

其中 α 是 x^2-x-1 的一个根．

3)　因 $25=5^2$，而 x^2+3 在 $\mathbb{Z}_5$上不可约(第十五章，三，4，3))，故

$$GF(25)=\mathbb{Z}_5(\alpha)=\{a_0+a_1\alpha\,|\,a_i\in\mathbb{Z}_5\},$$

其中 α 是 x^2+3 的一个根．

4)　因 $27=3^3$，而 x^3-x-1 在 $\mathbb{Z}_3$上不可约，故

$$GF(27)=\mathbb{Z}_3(\alpha)=\{a_0+a_1\alpha+a_2\alpha^2\,|\,a_i\in\mathbb{Z}_3\},$$

其中 α 是 x^3-x-1 的一个根．

5)　因 $32=2^5$，而 x^5+x^2+1 在 $\mathbb{Z}_2$上不可约，故

$$GF(32)=\mathbb{Z}_2(\alpha)=\left\{\sum_{i=0}^{4}a_i\alpha^i\,\middle|\,a_i\in\mathbb{Z}_2\right\},$$

其中 α 是 x^5+x^2+1 的一个根．

6)　因 $125=5^3$，而 x^3+x^2+x+3 在 $\mathbb{Z}_5$上不可约，故

$$GF(125)=\mathbb{Z}_5(\alpha)=\{a_0+a_1\alpha+a_2\alpha^2\,|\,a_i\in\mathbb{Z}_5\},$$

其中 α 是 x^3+x^2+x+3 的一个根．

注　在 1)中 $GF(4)$还可写成是 x^4-x 在 $\mathbb{Z}_2$上的分裂域，或写成是 $\mathbb{Z}_2[x]/(x^2+x+1)$．其余 2)—6)类同．

5. 有没有含 60 个或 100 个元的有限域?

解　因 $60=2^2\cdot3\cdot5$，$100=2^2\cdot5^2$，都不是 p^n 形，这里 p 是素数，n 是正整数，故没有

这样的有限域.

注 任给一个正整数 n,未必有含 n 个元的域,但必有含 p^n 个元的域,p 是素数.这是因为有限域的元的个数具有特殊的规律.

6. 判断以下各域 F 上的多项式 $f(x)$ 在其分裂域中有无重根.

1) $f(x)=x^2+1$. $F=\mathbb{Q}$.

2) $f(x)=x^2+1$. $F=\mathbb{Z}_2$.

3) $f(x)=x^3+2x+2$. $F=\mathbb{Z}_3$.

4) $f(x)=x^p-(p-1)$. $F=\mathbb{Z}_p$,p 是素数.

5) $f(x)=x^p-x-a$. $F=\mathbb{Z}_p$,p 是素数.

6) $f(x)=x^n-1$. ch $F=$素数 p,n 与 p 互素.

解 利用第十七章,一,11,1)来判断 $f(x)$ 是否有重根.

1) 因 $f'(x)=2x$,故 $f(x)$,$f'(x)$ 互素,从而 $f(x)$ 无重根.

2) 因 $f'(x)=2x=0$(由 ch $\mathbb{Z}_2=2$),故 $f(x)$,$f'(x)$ 不互素,从而 $f(x)$ 有重根.实际上,$x^2+1=x^2+1^2=(x+1)^2$,于是 $-1=1$ 是 x^2+1 的 2 重根.

3) 因 $f'(x)=3x^2+2=2$,故 $f(x)$,$f'(x)$ 互素,从而 $f(x)$ 无重根.

4) 因 ch $\mathbb{Z}_p=p$,故 $f'(x)=px^{p-1}=0$,于是 $f(x)$,$f'(x)$ 不互素.从而 $f(x)$ 有重根.由第十七章,二,4,若 α 是 $f(x)$ 的一个根,则 α 是 $f(x)$ 的 p 重根.

5) 因 $f'(x)=px^{p-1}-1=-1$,故 $f(x)$,$f'(x)$ 互素,从而 $f(x)$ 无重根.

6) 因 n 与 p 互素,故 $p\nmid n$,从而 $f'(x)=nx^{n-1}\neq 0$,于是 $f(x)$,$f'(x)$ 互素.所以 $f(x)$ 无重根.

四、思考问题

1. 设 E 是域 F 的代数扩域,且 F 上每一多项式($\in F$)在 F 上的分裂域都是 E 的子域,证明:E 是代数闭域.

2. 设 I 是域 F 的有限扩域,$f(x)$ 是 I 上不可约多项式.证明:存在 F 上不可约多项式 $g(x)$,使在 $I[x]$ 中,$f(x)\,\big|\,g(x)$.

3. 设 E 是域 F 上 $n(\geqslant 1)$ 次多项式 $f(x)$ 在 F 上的分裂域,证明:$(E:F)\leqslant n!$.

4. 1) 设 E 是含 $q=p^n$ 个元的有限域,ch $E=$素数 p.证明:E 中所有非零元的积是 -1(E 中单位元 1 的负元).

2) (威尔逊(Wilson)定理)若 p 是素数,证明:$(p-1)!\equiv -1(p)$.

5. 设 Δ 是特征为素数 p 的素域,α 是 Δ 上 n 次不可约多项式 $f(x)$ 的一个根.证明:$\alpha^p,\alpha^{p^2},\cdots,\alpha^{p^n}$ 都是 $f(x)$ 的根,且 $\alpha^{p^n}=\alpha$.

6. 设 G 是有限交换群.证明:

$$G\text{ 是循环群}\Leftrightarrow G\text{ 的阶 }|G|\text{ 是使 }a^n=e(\forall a\in G)\text{ 成立的最小正整数 }n\text{,这里 }e\text{ 是 }G\text{ 的单位元.}$$

7. 将下列各有理数域 $\mathbb{Q}$ 的有限扩域 E 表成 $\mathbb{Q}$ 的单扩域.

1) $E=\mathbb{Q}(\sqrt{2},\mathrm{i})$.

2)　$E=\mathbf{Q}(\sqrt{3},\sqrt[3]{2})$.

3)　$E=\mathbf{Q}(\sqrt[5]{2},\omega)$，其中 $\omega=\cos\frac{2\pi}{5}+\mathrm{i}\sin\frac{2\pi}{5}$.

4)　$E=\mathbf{Q}(\sqrt{2}\,\mathrm{i},\omega)$，其中 $\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}$.

5)　$E=\mathbf{Q}(\omega,2\mathrm{i})$，其中 $\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}$.

（见第十七章，一，17，注 4)，例.）

8. 1)　求出 $\sqrt{2}+\mathrm{i}$ 在 $\mathbf{R}$ 上极小多项式.

2)　求出 $\sqrt{2}+\mathrm{i}$ 在 $\mathbf{Q}$ 上极小多项式.

3)　求出 $\mathbf{Q}(\sqrt{2}+\mathrm{i})$ 在 $\mathbf{Q}$ 上的一个基.

4)　直接证明 $\mathbf{Q}(\sqrt{2},\mathrm{i})=\mathbf{Q}(\sqrt{2}+\mathrm{i})$.

（见第十七章，一，17，注 4)，例.）

9. 设 F 是域，$\mathrm{ch}\,F=\infty$，$f(x)$ 是 F 上最高系数为 1 的 $n(>0)$ 次多项式. 若 $d(x)=(f(x),f'(x))$，$f(x)=d(x)g(x)$，证明：$g(x)$ 有与 $f(x)$ 相同的根，且这些根就是 $g(x)$ 的所有的单根.

10. 设 F 是特征为素数 p 的域，$a\in F$，证明：

1)　$f(x)=x^p-x-a$ 没有重根.

2)　$f(x)$ 在 F 上不可约 $\Leftrightarrow a\neq c^p-c$，$\forall c\in F$（即 $f(x)=x^p-x-a$ 在 F 中没有根）.

思考问题解答

第一章

1. 解 1)—6) 都不能组成集合.

2. 解 1),2)错. 3)—15)对. 16)—19)错. 20)对. 21)—23)错. 24)—26)对. 27)错.

3. 解 4).

4. 解 因 $A_0 \supset A_1 \supset A_2 \supset \cdots$,故 $\bigcup\limits_{i=0}^{+\infty} A_i = A_0 \cup A_1 \cup A_2 \cup \cdots = A_0$. 因 $\forall x \in \mathbf{R}$,$\exists$ 非负整数 n,使得 $x \leqslant n$,于是 $x \overline{\in} A_n$,故 $x \overline{\in} \bigcap\limits_{i=0}^{+\infty} A_i$,所以 $\bigcap\limits_{i=0}^{+\infty} A_i = \varnothing$.

5. 解 $\bigcup\limits_{i=1}^{+\infty} A_i = A_1$, $\bigcap\limits_{i=1}^{+\infty} A_i = \{0\}$.

6. 证 ($\Rightarrow$) 因 $A \cup B = A \cup A = A$, $A \cap B = A \cap A = A$,故 $A \cup B \subset A \cap B$. ($\Leftarrow$) $\forall x \in A$,有 $x \in A \cup B \subset A \cap B \subset B$,从而 $A \subset B$;同理 $B \subset A$. 所以 $A = B$.

7. 解 解不等式得 $A = (-4,4)$, $B = (-\infty,1] \cup [3,+\infty)$,于是

$$\begin{aligned} A \cap B &= (-4,4) \cap \big((-\infty,1] \cup [3,+\infty)\big) \\ &= \big((-4,4) \cap (-\infty,1]\big) \cup \big((-4,4) \cap [3,+\infty)\big) \\ &= (-4,1] \cup [3,4). \end{aligned}$$

8. 证 1) 设 $f(x)g(x)$ 的实根的集合为 C,要证 $C = A \cup B$. $\forall \alpha \in C$,则 $f(\alpha)g(\alpha) = 0 \Rightarrow f(\alpha) = 0$ 或 $g(\alpha) = 0 \Rightarrow \alpha \in A$ 或 $\alpha \in B \Rightarrow \alpha \in A \cup B$;反之,$\forall \alpha \in A \cup B$,则 $\alpha \in A$ 或 $\alpha \in B \Rightarrow f(\alpha) = 0$ 或 $g(\alpha) = 0 \Rightarrow f(x)g(\alpha) = 0 \Rightarrow \alpha \in C$. 所以 $C = A \cup B$.

2) 设 $f^2(x) + g^2(x)$ 实根的集合为 C,要证 $C = A \cap B$. $\forall \alpha \in C \Rightarrow f^2(\alpha) + g^2(\alpha) = 0$. 因 $f^2(\alpha)$, $g^2(\alpha)$ 都是非负实数,故 $f^2(\alpha) = g^2(\alpha) = 0 \Rightarrow f(\alpha) = g(\alpha) = 0 \Rightarrow \alpha \in A$ 且 $\alpha \in B \Rightarrow \alpha \in A \cap B$;反之,$\forall \alpha \in A \cap B \Rightarrow \alpha \in A$ 且 $\alpha \in B \Rightarrow f(\alpha) = g(\alpha) = 0 \Rightarrow f^2(\alpha) = g^2(\alpha) = 0 \Rightarrow f^2(\alpha) + g^2(\alpha) = 0 \Rightarrow \alpha \in C$. 所以 $C = A \cap B$.

9. 解 当 n 是偶数时,取 A_1 与 A_2 使其所含元的个数都是 $\frac{n}{2}$,于是 $A_1 \times A_2$ 含 $\frac{n}{2} \cdot \frac{n}{2} = \frac{n^2}{4}$ 个元,个数最大;当 n 是奇数时,取 A_1 含 $\frac{n+1}{2}$ 个元,则 A_2 含 $n - \frac{n+1}{2} = \frac{n-1}{2}$ 个元,于是 $A_1 \times A_2$ 含 $\frac{n+1}{2} \cdot \frac{n-1}{2} = \frac{n^2-1}{4}$ 个元,个数最大.

10. 解 1)是. 2),3)不是. 4)是. 5)—11)不是. 12)是.

11. 解 1),2)都是 $\phi_1 = \phi_2$.

12. 解 1)—7)不是． 8)—12)是.

13. 解 因 A 的一个代数运算就是 $A\times A$ 到 A 的一个映射，而 $A\times A$ 恰含 n^2 个元，A 恰含 n 个元，从而 $A\times A$ 到 A 的映射共有 n^{n^2} 个．所以 A 中最多有 n^{n^2} 种代数运算(见第一章，三，4).

14. 解 5 种.

15. 解 1) 适合交换律，不适合结合律．2) 结合律和交换律都不适合．3) 适合结合律，不适合交换律．4) 结合律和交换律都不适合.

16. 证 因表中主对角线两侧对称位置元素相同，故・适合交换律，可不考虑顺序．又表中第一行、第一列分别与表头的行、列相同，说明 $\forall x\in A$，都有 $ax=x=xa$. 再者表中主对角线上的元素都是 a，因此，$\forall x\in A$，都有 $xx=a$. 下面证明：$\forall x,y,z\in A$，都有 $(xy)z=x(yz)$. 分四种情况：

1) x,y,z 中有 a 时，显然 $(xy)z=x(yz)$.

2) x,y,z 中无 a，且它们互不相同时，从表中可看出，x,y,z 中任意两个元的乘积是第三个元，即 $xy=z,yz=x$，从而

$$(xy)z=zz=a,\quad x(yz)=xx=a.$$

所以 $(xy)z=x(yz)$.

3) x,y,z 中无 a，且 $x=y=z$ 时，

$$(xy)z=(xx)x=ax=x,$$
$$x(yz)=x(xx)=xa=x.$$

所以 $(xy)z=x(yz)$.

4) x,y,z 中无 a，且其中恰有两个元素相同时，设这个相同元素与另一个元素乘积是 u.

① 若 $x=y,(xy)z=(xx)z=az=z,x(yz)=xu=z$.

② 若 $x=z,(xy)z=uz=y,x(yz)=xu=y$.

③ 若 $y=z,(xy)z=uz=x,x(yz)=x(yy)=xa=x$.

总之，此时有 $(xy)z=x(yz)$.

综上所述，该代数运算适合结合律.

17. 证 命题："若 $a\neq b$，有 $a\circ b\neq b\circ a$"的逆否命题："若 $a\circ b=b\circ a$，有 $a=b$"成立.

1) $\forall a\in A,a\circ a\in A$，且 $(a\circ a)\circ a=a\circ(a\circ a)$，所以 $a\circ a=a$.

2) $\forall a,b\in A,(a\circ b\circ a)\circ a=(a\circ b)\circ(a\circ a)=(a\circ b)\circ a=a\circ(b\circ a)=(a\circ a)\circ(b\circ a)=a\circ(a\circ b\circ a)$，所以 $a\circ b\circ a=a$.

3) $\forall a,b,c\in A,(a\circ b\circ c)\circ(a\circ c)=(a\circ b)\circ(c\circ a\circ c)=(a\circ b)\circ c=a\circ(b\circ c)=(a\circ c\circ a)\circ(b\circ c)=(a\circ c)\circ(a\circ b\circ c)$，所以 $a\circ b\circ c=a\circ c$.

18. 证 $(a\circ b)\circ(a\circ b)=a\circ(b\circ a)\circ b=a\circ(a\circ b)\circ b=(a\circ a)\circ(b\circ b)=a\circ b$.

19. 解 1) $\forall a,b,c\in A$. 2) $(a_1,a_2),i=1,2$. 3) $a_1,a_2,\cdots,a_n,i=1,2,\cdots,n$. 4) $a\neq 0,b\neq 0$.

第二章

1. 解 1) $\phi:n\rightarrow 1$. 2) $\phi:n\rightarrow n$. 3)不存在． 4) $\phi:n\rightarrow 1$. 5) $\phi:n\rightarrow n,n<5$ 时；

$n \to n-1, n=5$ 时．6)不存在.

2. 解 1) ϕ未必是满射,因为未必每个年级都有学生．一般说ϕ不是单射,因为某年级如有学生,一般不会只有一个人．2) ϕ不是满射．ϕ不是单射．3) ϕ不是满射,也不是单射．4) ϕ不是满射．ϕ是单射．5) ϕ是满射,但不是单射．6) ϕ不是满射,也不是单射．7) ϕ不是满射,也不是单射．8) ϕ不是映射,因而既不是满射,也不是单射．9) ϕ是满射,但不是单射．10) ϕ是满射,但不是单射．11) ϕ是满射,而不是单射.

3. 解 因ϕ是A到B的单射,故A中k个元在ϕ下的象是B中k个不同的元．于是ϕ的个数是从B中n个元每次取k个不同的元进行排列所得到的排列数,即A到B的单射的个数为

$$p_n^k = n(n-1)(n-2)\cdots(n-k+1) = \frac{n!}{(n-k)!}.$$

4. 证 1) $\forall g(x) \in A$,令$g(x)=(x^2+1)f(x)$,则因$x^2+1 \neq 0$,故$f(x)=\frac{g(x)}{x^2+1}$,从而$\exists \frac{g(x)}{x^2+1} \in A$,使得

$$\phi\left(\frac{g(x)}{x^2+1}\right) = (x^2+1)\frac{g(x)}{x^2+1} = g(x).$$

所以ϕ是满射．又$\forall f(x), g(x) \in A$,若$(x^2+1)f(x)=(x^2+1)g(x)$,因$x^2+1 \neq 0$,故$\exists \frac{1}{x^2+1} \in A$,使得

$$\frac{1}{x^2+1}(x^2+1)f(x) = \frac{1}{x^2+1}(x^2+1)g(x) \Rightarrow f(x)=g(x).$$

所以ϕ是单射.

2) $\forall m \in B$,当m是非负偶数时,m在ϕ下的逆象是$\frac{m}{2} \in A$. 当m是非负奇数时,可写成$m=-(2n+1)$,其中$n<0$,则m在ϕ下的逆象是$n \in A$. 所以ϕ是满射．又$\forall n, m \in A$,当n, m都$\geqslant 0$时,若$2n=2m$,有$n=m$. 当n, m都<0时,若$-2n-1=-2m-1$,有$n=m$. 当$n \geqslant 0, m<0$时,则$n \neq m$,有$2n \neq -2m-1$. 当$m \geqslant 0, n<0$时,则$m \neq n$,有$2m \neq -2n-1$. 所以ϕ是单射.

5. 解 1) $\phi: 2n-1 \to 2n, n=1,2,\cdots,50$. 2) $\phi: n \to n-1$. 3) $\phi: n \to n+1$.

4) 非负整数集B是A的一个子集．$\phi: \begin{cases} n \to n+1 (n \in B); \\ x \to x (x \in A-B). \end{cases}$

5) $\phi: \begin{cases} x_n \to 2n-1; \\ y_n \to 2n, \end{cases} n=1,2,\cdots$ 6) $\phi: \begin{cases} n \to 2n+2, \text{当 } n \geqslant 0 \text{ 时}; \\ n \to -2n-1, \text{当 } n<0 \text{ 时}. \end{cases}$ 7) $\phi: x \to \frac{x}{1+x}$.

8) $\phi: x \to \frac{x}{1-x}$.

6. 解 1) $\phi^{-1}: x \to \frac{x}{2}-\frac{1}{2}$. 2) $\phi^{-1}: X \to X'$. 3) $\phi^{-1}: y \to -\sqrt{y}$.

4) $\phi^{-1}: y \to \frac{b-a}{d-c}(y-c)+a$.

7. 证 1) 对于$\circ$和$\bar{\circ}$来说,存在A到$\overline{A}$的同态满射$\phi: \begin{cases} n \to -1, n<0 \text{ 时}; \\ n \to 0, n=0 \text{ 时}; \\ n \to 1, n>0 \text{ 时}. \end{cases}$

2） 对于$\circ$和$\bar{\circ}$来说，存在A到$\overline{A}$的同态满射$\phi: a+b\mathrm{i}\to a$.

3） 对于$\circ$和$\bar{\circ}$来说，存在A到$\overline{A}$的同态满射$\phi: 1\to 1, \mathrm{i}\to -1, -1\to 1, -\mathrm{i}\to -1$. 4) $\forall x\in A$，都有$x=2^k\cdot\frac{p}{q}$，其中p,q都是奇数．可以证明：对于$\circ$和$\bar{\circ}$来说，存在A到$\overline{A}$的同态满射ϕ：$x\to k$.

8. 证 取$1+\sqrt{2},\sqrt{2}\in A$，则$\phi: 1+\sqrt{2}\to 1+\sqrt{3}$，而$\sqrt{2}\to\sqrt{3}$，从而$\phi: (1+\sqrt{2})\sqrt{2}=2+\sqrt{2}\to 2+\sqrt{3}$，但$(1+\sqrt{3})\sqrt{3}=3+\sqrt{3}$，所以$\phi((1+\sqrt{2})\sqrt{2})\neq\phi(1+\sqrt{2})\phi(\sqrt{2})$.

9. 证 1） 假设A与$\overline{A}$间有同构映射，设为ϕ．对于$1\in\overline{A}$，因ϕ是满射，故$\exists a\in A$，使得$\phi(a)=1$. 对于$\frac{a}{2}\in A$，因ϕ是映射，故$\exists n\in\overline{A}$，使得$\phi\left(\frac{a}{2}\right)=n$. 因$\phi$保持运算，故

$$1=\phi(a)=\phi\left(\frac{a}{2}+\frac{a}{2}\right)=\phi\left(\frac{a}{2}\right)+\phi\left(\frac{a}{2}\right)=n+n=2n,$$

从而$n=\frac{1}{2}$，但$\frac{1}{2}\,\overline{\in}\,\overline{A}$，即$\frac{a}{2}\in A$在$\phi$下在$\overline{A}$中无象，此与$\phi$是映射矛盾．因此$A\not\cong\overline{A}$.

注 将A改为实数集，$\overline{A}$改为自然数集，同样可证$A\not\cong\overline{A}$.

2） 设ϕ是A与$\overline{A}$间的一个同构映射．由ϕ是映射，可设$\phi: 1\to a$. 由ϕ保持运算，有ϕ：$1\cdot 1\to a+a$. 因$1=1\cdot 1$，ϕ是映射，故$a=a+a=2a$，从而$a=0$，即$\phi: 1\to 0$. 由ϕ是映射，可设$\phi: -1\to b$. 因ϕ是单射，故$b\neq 0$. 由ϕ保持运算，有

$$2b=b+b=\phi(-1)+\phi(-1)=\phi((-1)(-1))=\phi(1)=0.$$

即$b=0$，得出矛盾．所以$A\not\cong\overline{A}$.

10. 解 不对.

1） **例** 取$A=\mathbf{R}$，$\overline{A}=\{1\}$. $a\circ b=\frac{a+b}{2}$，$\bar{a}\,\bar{\circ}\,\bar{b}=\bar{a}\,\bar{b}$. $\phi: a\to 1$. 都合乎题中的条件．显然$\bar{\circ}$适合结合律，但$\circ$不适合结合律.

2） **例** 取$A=\mathbf{R}^+$，$\overline{A}=\{1\}$. $a\circ b=\frac{a}{b}$，$\bar{a}\,\bar{\circ}\,\bar{b}=\bar{a}\,\bar{b}$. $\phi: a\to 1$. 都符合条件．显然$\bar{\circ}$适合交换律，但$\circ$不适合交换律.

11. 解 不对.

1） **例** 取$A=\mathbf{R}^+$，$\overline{A}=\{0\}$. $a\odot b=\frac{a}{b}$，$a\oplus b=a+b$. $a\,\overline{\odot}\,b=ab$. $a\,\overline{\oplus}\,b=a+b$. $\phi: a\to 0$. 都适合条件．显然$\overline{\odot}$，$\overline{\oplus}$适合第一分配律，但$\odot$，$\oplus$不适合第一分配律.

2） **例** 将1)中例$a\odot b$改为$\frac{b}{a}$，其余不动．显然$\overline{\odot}$，$\overline{\oplus}$适合第二分配律，但$\odot$，$\oplus$不适合第二分配律(见第一章，三，7).

第三章

1. 解 1） 是．A中任意两个元的和都$\not<0$，故A中任意两个元都不符合关系R，这样的关系R叫空关系.

2） 是．A中任意两个元都符合关系R，这样的关系叫全关系.

3) 不是．取$\frac{2}{3},\frac{1}{2}\in A$,因 $2>1$,故

$$R:\left(\frac{2}{3},\frac{1}{2}\right)\to \text{对}.$$

但$\frac{1}{2}=\frac{3}{6}$,而 $2\not>3$,故

$$R:\left(\frac{2}{3},\frac{1}{2}\right)\to \text{错}.$$

从而 R 不是 $A\times A$ 到 D 的映射．如果将上面的$\frac{b}{a},\frac{d}{c}$限定为既约分数,那么,R 就是 A 的元间的一个关系.

2. 解 1) $A_0,A_1,A_2,\cdots$不是 A 的一个分类．因为零多项式 0 没有次数,所以 $0\overline{\in}$某 A_i. $\{0\},A_0,A_1,A_2,\cdots$是 A 的一个分类.

2) A_1,A_2,A_3 不是 A 的一个分类．如恒等变换 $\varepsilon:a\to a$,它既属于 A_1,又属于 A_2,从而 $A_1\cap A_2\neq\varnothing$.

3. 解 1)不是． 2)不是． 3)不是． 4)不是． 5)是． 6)不是． 7)不是.

4. 证 1) 因 $n\,|\,a-b,n\,|\,c-d$,故 $n\,|\,a-b\pm(c-d)\Rightarrow n\,|\,a\pm c-(b\pm d)\Rightarrow a\pm c\equiv b\pm d(n)$.

2) 因 $n\,|\,a-b$,故 $n\,|\,m(a-b)\Rightarrow n\,|\,ma-mb\Rightarrow ma\equiv mb(n)$.

3) 因 $n\,|\,a-b,n\,|\,c-d$,故 $n\,|\,c(a-b),n\,|\,b(c-d)\Rightarrow n\,|\,ac-cb,n\,|\,bc-bd\Rightarrow n\,|\,ac-cb+bc-bd=ac-bd\Rightarrow ac\equiv bd(n)$.

5. 解 1) 由～决定的含元素 $a+b\mathrm{i}$ 的类是

$$[a+b\mathrm{i}]=\left\{c+d\mathrm{i}\in A\,\middle|\,a^2+b^2=c^2+d^2\right\}.$$

这样的类的全体就是 A 的一个分类．从几何意义上来看,类$[a+b\mathrm{i}]$中的元是在复平面上以原点为圆心,以 $a^2+b^2=r$ 为半径的圆．由～决定的 A 的分类是复平面上以原点为圆心的一系列的圆.

2) 由～决定的含元素 $x\neq0$ 的类是

$$[x]=\left\{y\in A\,\middle|\,y^2=x^2\right\}=\left\{x,-x\right\}.$$

而含 0 的类是

$$[0]=\left\{y\in A\,\middle|\,y^2=0^2\right\}=\left\{0\right\}.$$

这些类的全体就是 A 的一个分类.

3) 由～决定的含元素 X 的类是

$$[X]=\left\{Y\in A\,\middle|\,\exists\ \text{可逆矩阵}\ P\in A,\text{使得}\ PY=X\right\},$$

即类$[X]$中恰含经行的初等变换可化为矩阵 X 的一切矩阵．这些类的全体就是 A 的一个分类.

4) 由～决定的含元素 X 的类是

$$[X]=\left\{Y\in A\,\middle|\,|Y|=|X|=a\in\mathbf{R}\right\},$$

即类$[X]$是由 A 中一切行列式值为$|X|=a$ 的矩阵所作成．这些类的全体就是 A 的一

个分类.

5) 由～决定的含元素 X 的类是

$$[X]=\left\{Y\in A\,\middle|\,Y\text{ 与 }X\text{ 相似}\right\}.$$

所有这样的类作成 A 的一个分类.

6) 由～决定的含元素 X 的类是

$$[X]=\left\{Y\in A\,\middle|\,\text{秩 }Y=\text{秩 }X=r\right\}.$$

因此,

$$A_0=\left\{Y\in A\,\middle|\,\text{秩 }Y=0\right\}=\{0\},$$

$$A_1=\left\{Y\in A\,\middle|\,\text{秩 }Y=1\right\},$$

$$A_2=\left\{Y\in A\,\middle|\,\text{秩 }Y=2\right\},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$A_n=\left\{Y\in A\,\middle|\,\text{秩 }Y=n\right\}$$

是 A 的一个分类.

7) 由～决定的含元素(x_1,y_1)的类是

$$[(x_1,y_1)]=\left\{(x_2,y_2)\in A\,\middle|\,x_2x_1>0\text{ 且 }y_2y_1>0\right\},$$

即与点(x_1,y_1)在同一象限的所有的点作成了类$[(x_1,y_1)]$. 从而 A_1,A_2,A_3,A_4 是 A 的一个分类,其中 A_i 是第 i 象限的所有的点作成的集合,$i=1,2,3,4$.

8) 由～决定的含元素 x 的类是

$$[x]=\left\{y\in A\,\middle|\,[y]=[x]\right\},$$

从而,$\cdots,A_{-2},A_{-1},A_0,A_1,A_2,\cdots$是 A 的一个分类,其中 $A_i=[i,i+1)$,$i=0,\pm1,\pm2,\cdots$

注 不是等价关系的关系不能决定集 A 的一个分类. 例,$a\,|\,b$ 是整数集 $\mathbb{Z}$ 的元间的一个关系,但不是等价关系. 含 4 的类是$[4]=\left\{x\in\mathbb{Z}\,\middle|\,x|4\right\}$,于是 $2\in[4]$,从而$[2]=[4]$,但 $4\overline{\in}[2]=\left\{x\in\mathbb{Z}\,\middle|\,x|2\right\}$,此与$[2]=[4]$矛盾.

第四章

1. 解 1)是. -1 是单位元,$a(\neq0)$的逆元是$\frac{1}{a}$.

2) 是. 2 是单位元,a 的逆元是$\frac{4}{a}$.

3) 是. $-\frac{1}{n}$是单位元,a 的逆元是$\frac{1}{n^2a}$.

4) 不是. ∘不适合结合律.

5) 不是. ∘不适合结合律.

6) 是. 单位元、逆元不变.

7) 是. u^{-1}是单位元,a 的逆元是 $u^{-1}a^{-1}u^{-1}$.

8） 是．2 是单位元，a 的逆元是 $4-a$.

9） 是．3 是单位元，a 的逆元是 $6-a$.

10） 是．首先$\circ$是一个代数运算．事实上，$\forall a,b\in\mathbb{Q}-\{-1\}$，即 $a\neq-1,b\neq-1$. 如果 $a\circ b=a+b+ab=-1$，那么 $(1+a)b=-(1+a)$. 因 $a\neq-1$，故 $1+a\neq0$，从而可由上式两端消去 $1+a$，得 $b=-1$，此为不可能．所以 $a\circ b\neq-1$，即 $a\circ b\in\mathbb{Q}-\{-1\}$，因此 $\mathbb{Q}-\{-1\}$ 对$\circ$封闭．0 是单位元．a 的逆元是 $-\dfrac{a}{1+a}$.

11） 不是．0 是单位元．但 1 在 $\mathbb{Z}$ 中无逆元.

12） 是．1 是单位元．当 $a>0$ 时，a 的逆元是 $\dfrac{1}{a}$；当 $a<0$ 时，a 的逆元是 a.

13） 不是．取 $\dfrac{1-t}{t},\dfrac{t}{1-t}\in G$，有

$$\frac{1-t}{t}\circ\frac{t}{1-t}=\frac{1-\dfrac{t}{1-t}}{\dfrac{t}{1-t}}=\frac{\dfrac{1-t-t}{1-t}}{\dfrac{t}{1-t}}=\frac{1-2t}{1-t}\cdot\frac{1-t}{t}=\frac{1-2t}{t}\overline{\in}G,$$

所以$\circ$不是 G 的一个代数运算.

14） 是．$(0,0)$是单位元，(a,b)的逆元是$(-a,-b)$.

15） 是．若 e 是 G 的单位元，则(e,e)是 $G\times G$ 的单位元．(a,b)的逆元是(a^{-1},b^{-1}).

16） 是．$(0,0)$是 G 的单位元．(a,b)的逆元是$(-ae^{b},-b)$.

17） 不是．空集$\varnothing$是 $P(A)$的单位元．但 $A(\in P(A))$无逆元.

18） 不是．A 是 $P(A)$的单位元．但空集$\varnothing(\in P(A))$无逆元.

19） 是．u 是单位元．a 的逆元是 $ua^{-1}u$.

20） 不是．因为若 $f(x)\in G$，而次 $f(x)\geqslant1$，则 $f(x)$在 G 中无逆元.

（此 G 说明，对于无限集合来说，虽对于乘法封闭，适合结合律和消去律，但此无限集合未必能作成一个群．）

21） 是．零映射是单位元．映射 f 的逆元是 f 的逆映射 $-f$.

22） 是．$\begin{pmatrix}1&0\\0&1\end{pmatrix}$是单位元．每个元的逆元都是自身.

23） 是．$e=\begin{pmatrix}1&0\\0&1\end{pmatrix}$是单位元．$e,a,b,c$ 的逆元都是自身．d 与 f 互为逆元.

24） 是．$\begin{pmatrix}1&0\\0&0\end{pmatrix}$是单位元．$\begin{pmatrix}a&0\\0&0\end{pmatrix}$的逆元是$\begin{pmatrix}\dfrac{1}{a}&0\\0&0\end{pmatrix}$.

25） 是．$\begin{pmatrix}0&0\\0&0\end{pmatrix}$是单位元．$\begin{pmatrix}a&2b\\b&a\end{pmatrix}$的逆元是$\begin{pmatrix}-a&2(-b)\\-b&-a\end{pmatrix}$.

26） 不是．$\begin{pmatrix}0&0\\0&0\end{pmatrix}(\in G)$没有逆元.

27） 是．$e=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$是单位元．$e,a,b,c$ 的逆元都是自身．d 与 f 互为逆元.

28） 不是．取$\begin{pmatrix}1&0\\0&1\end{pmatrix}$，$\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\in G$，但$\begin{pmatrix}1&0\\0&1\end{pmatrix}+\begin{pmatrix}-1&0\\0&-1\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}\overline{\in} G$，从而$G$对加法不封闭.

29） 是．n阶零矩阵是单位元．n阶实矩阵A的逆元是$-A$.

30） 是．零向量是单位元．向量α的逆元是α的负向量.

31） 是．空集$\varnothing$是单位元．每个元都以它自身为逆元．运算表是

$\circ$	$\varnothing$	$\{a\}$	$\{b\}$	A
$\varnothing$	$\varnothing$	$\{a\}$	$\{b\}$	A
$\{a\}$	$\{a\}$	$\varnothing$	A	$\{b\}$
$\{b\}$	$\{b\}$	A	$\varnothing$	$\{a\}$
A	A	$\{b\}$	$\{a\}$	$\varnothing$

32） 是．运算表是

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_6	f_4	f_5
f_3	f_3	f_1	f_2	f_5	f_6	f_4
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

$f_1(x)$是单位元．f_1，f_4，f_5，f_6的逆元都是自身，f_2和f_3互为逆元.

33） 不是．12是单位元，但1，2，3，4，6都没有逆元.

34） 是．

$$(a\circ b)\circ c=\begin{cases}(a+b)\circ c=\begin{cases}a+b+c, a\text{偶}, b\text{偶},\\ a+b-c, a\text{偶}, b\text{奇}.\end{cases}\\ (a-b)\circ c=\begin{cases}a-b+c, a\text{奇}, b\text{奇},\\ a-b-c, a\text{奇}, b\text{偶}.\end{cases}\end{cases}$$

$$a\circ(b\circ c)=\begin{cases}a\circ(b+c)=\begin{cases}a+b+c, a\text{偶}, b\text{偶},\\ a-b-c, a\text{奇}, b\text{偶}.\end{cases}\\ a\circ(b-c)=\begin{cases}a+b-c, a\text{偶}, b\text{奇},\\ a-b+c, a\text{奇}, b\text{奇}.\end{cases}\end{cases}$$

所以，$(a\circ b)\circ c=a\circ(b\circ c)$．0是单位元．任一偶数$a$的逆元是$-a$，任一奇数$a$的逆元就是$a$本身.

35） 是．4阶单位矩阵是单位元．每个元的逆元都是自身.

2. 证 ① 若$a\neq e$，由3)，$\exists a'\in G$，使得$aa'=e$，于是$a'\neq e$. 假定不然，$a'=e$，由1)，有$aa'=ae=a$，从而$a=e$，矛盾.

② 若$a\neq e$，$\exists a'\in G$，使得$aa'=e$，由①$a'\neq e$. 对于$a'\neq e$，$\exists a''\in G$，使得$a'a''=e$，由①，$a''\neq e$. 对于$a''\neq e$，$\exists a'''\in G$，使得$a''a'''=e$，由①，$a'''\neq e$. 于是

$$e=aa'\xlongequal{\text{由 1)}}a(a'e)=a(a'(a''a'''))$$

$$\xlongequal{\text{由 2)}} a\big((a'a'')a'''\big) \xlongequal{\text{由 2)}} \big(a(a'a'')\big)a'''$$
$$= \big((aa')a''\big)a''' = (aa')(a''a''')$$
$$= e^2,$$

从而 1)与 3)中的条件 $a\neq e$ 可以去掉．这样，G 就有右单位元，且 $\forall a\in G$，a 在 G 中都有右逆元．又因 $a(be)=ab$，且 $(ab)e=ab$，故 $\forall a,b,c\in G$，都有 $a(bc)=(ab)c$，即结合律成立．所以 G 对于这个乘法作成一个群.

3. 证 设 e 是 $ya=a$ 在 G 中的唯一解，则 e 是 G 的左单位元．因为，$\forall b\in G$，都 $\exists x\in G$，使得 $ax=b$，于是 $eb=e(ax)=(ea)x=ax=b$，即 e 是 G 的一个左单位元.

又 $ya=a$ 仅有一解，故 G 有唯一的一个左单位元 e. $\forall a\in G$，由于方程 $ax=e$ 在 G 中有解，故 $\exists a$ 的右逆元 $a'\in G$，使得 $aa'=e$，可证 a' 也是 a 的左逆元．事实上，命 a'' 是 a' 的一个右逆元，即 $a'a''=e$. 考虑 $a'a$，由于对任意 $x\in G$，均有

$$(a'a)x=(a'a)ex=(a'a)(a'a'')x=\big(a'(aa')\big)a''x(a'e)a''x=\big(a'(ea'')\big)x=(a'a'')x=ex=x,$$

即 $a'a$ 是 G 的一个左单位元．因已知方程 $ya=a$ 在 G 中有唯一解，故 G 有唯一的一个左单位元 e，于是 $a'a=e$，从而 a 有左逆元 $a'\in G$，即Ⅰ，Ⅱ，Ⅳ，Ⅴ都成立，所以 G 是一个群.

4. 证 (⇒) 因 G 是交换群，故

$$(ab)^2=abab=aabb=a^2b^2.$$

(⇐) 因 $\forall a,b\in G$，$(ab)^2=a^2b^2$，故 $abab=aabb$，由消去律，$ba=ab$.

5. 证 (⇒) $a^2=a\Rightarrow \exists a^{-1}\in G$，使得 $a^{-1}a^2=a^{-1}a\Rightarrow a=e$.

(⇐) $a=e$，因 $e^2=e$，故 $a^2=a$.

（即群中的幂等元有且只有单位元．）

6. 证 因 G 是群，故对于 $a,b\in G$，$\exists a^{-1},b^{-1}\in G$. 令 $x=a^{-1}bca^{-1}b^{-1}$，直接验证可知 $a^{-1}bca^{-1}b^{-1}$ 是方程 $xaxba=xbc$ 的一个解．故方程有解.

若 x_0 是方程 $xaxba=xbc$ 在 G 中的一个解，则由 $x_0ax_0ba=x_0bc$ 及消去律得 $ax_0ba=bc$，由此得 $x_0=a^{-1}bca^{-1}b^{-1}$. 所以方程 $xaxba=xbc$ 在 G 中只有一个解.

7. 证 $(a^{-1}ba)^k=a^{-1}ba$

$$\Leftrightarrow \overbrace{(a^{-1}ba)(a^{-1}ba)\cdots(a^{-1}ba)}^{k个}=a^{-1}ba$$
$$\Leftrightarrow a^{-1}b^ka=a^{-1}ba$$
$$\Leftrightarrow b^k=b.$$

8. 证 $\forall x\in G$，则 $|x^{-1}ax|=|a|$. 事实上，设 $|a|=n$，则

$$(x^{-1}ax)^n=\overbrace{(x^{-1}ax)(x^{-1}ax)\cdots(x^{-1}ax)}^{n个}=x^{-1}a^nx=x^{-1}ex=e,$$

从而

$$|x^{-1}ax|\leqslant n=|a|.$$

又设 $|x^{-1}ax|=m$，则

$$a^m=(xx^{-1}axx^{-1})^m=x(x^{-1}ax)^mx^{-1}$$
$$=xex^{-1}=e,$$

从而

$$|a| \leqslant m = |x^{-1}ax|.$$

所以$|x^{-1}ax|=|a|$. 而$|a|=2$,于是由题设有 $x^{-1}ax=a$,即 $ax=xa$.

注 直接利用$|ab|=|ba|$可得

$$|x^{-1}ax|=|x^{-1}xa|=|ea|=|a|.$$

或:$\forall x\in G, x^{-1}ax\neq e$. 不然,若 $x^{-1}ax=e$,则 $ax=x$,由消去律,$a=e$,此与$|a|=2$矛盾. 又

$$(x^{-1}ax)^2=(x^{-1}ax)(x^{-1}ax)=x^{-1}a^2x=e,$$

所以$|x^{-1}ax|=2=|a|$.

9. 证 $b^{-1}\circ a=(b^{-1}\circ a)\circ e=(b^{-1}\circ a)\circ(b\circ b^{-1})$

$$\begin{aligned}&=b^{-1}\circ\big(a\circ(b\circ b^{-1})\big)=b^{-1}\circ\big((a\circ b)\circ b^{-1}\big)\\&=b^{-1}\circ\big((b\circ a)\circ b^{-1}\big)=b^{-1}\circ\big(b\circ(a\circ b^{-1})\big)\\&=(b^{-1}\circ b)\circ(a\circ b^{-1})=e\circ(a\circ b^{-1})=a\circ b^{-1}.\end{aligned}$$

10. 证 (反证法)若 $ab=ba$,则

$$\begin{aligned}a^4b=ba^5&=(ba)a^4=(ab)a^4=a(ba)a^3\\&=a(ab)a^3=a^2(ba)a^2=a^2(ab)a^2\\&=a^3(ba)a=a^3(ab)a=a^4(ba)\\&=a^4(ab)=a^5b.\end{aligned}$$

由消去律,$e=a$,此与已知条件矛盾. 所以,$ab\neq ba$.

11. 证 $\forall a,b\in G$,

$$(ba)^\tau=(ba)^3=bababa.$$

$$(ba)^\tau=b^\tau a^\tau=b^3a^3$$

$$\Rightarrow b^3a^3=bababa$$

$$\xRightarrow{\text{消去律}} b^2a^2=abab. \qquad (*)$$

$$(a^2b^2)^\tau=(a^2b^2)^3=a^2b^2a^2b^2a^2b^2.$$

$$(a^2b^2)^\tau=a^{2^\tau}b^{2^\tau}=a^6b^6$$

$$\Rightarrow a^6b^6=a^2b^2a^2b^2a^2b^2$$

$$\xRightarrow{\text{消去律}} a^4b^4=b^2a^2b^2a^2$$

$$\xlongequal{(*)} abababab$$

$$\xRightarrow{\text{消去律}} a^3b^3=(ba)^3$$

$$\Rightarrow a^\tau b^\tau=(ba)^\tau$$

$$\Rightarrow (ab)^\tau=(ba)^\tau.$$

因 τ 是单射,故 $ab=ba$,所以 G 是交换群.

第五章

1. 解 1) 不正确. 例,$\phi: a\to\bar{e}$ 是群 G 到群 $\overline{G}$ 的一个同态映射,其中 $\overline{G}=\{\bar{e}\}$,而

$$G=\{\tau_{ab}\mid\forall x\in A, x^{\tau_{ab}}=ax+b, a\neq 0, a,b\text{ 是有理数}\},$$

A 是实数集．$\tau_{11},\tau_{20}\in G$，有$\phi(\tau_{11})\phi(\tau_{20})=\bar{e}\bar{e}=\phi(\tau_{20})\phi(\tau_{11})$，但 $\tau_{11}\tau_{20}=\tau_{22}\neq\tau_{21}=\tau_{20}\tau_{11}$．

2) ① 正确．事实上，$\forall y\in\mathbf{R}^+$，令 $y=2^{x-1}$，有 $\log_2 y=\log_2 2^{x-1}=x-1$，从而 $x=\log_2 y+1$．因此，$\exists x=\log_2 y+1\in\mathbf{R}$，使得$\phi: x=\log_2 y+1\to 2^{\log_2 y+1-1}=y$．所以$\phi$是满射．又 $\forall x,y\in\mathbf{R}$，$\phi: x\to 2^{x-1}$，$y\to 2^{y-1}$．若 $2^{x-1}=2^{y-1}$，则 $\log_2 2^{x-1}=\log_2 2^{y-1}$，从而 $x-1=y-1$，即 $x=y$．所以ϕ是单射．于是ϕ是$\mathbf{R}$与$\mathbf{R}^+$间的一个一一映射．

② 不正确．事实上，取 $1,2\in\mathbf{R}$，则$\phi: 1\to 2^{1-1}=1$，$2\to 2^{2-1}=2$，$1+2=3\to 2^{3-1}=4\neq 1\cdot 2$，即$\phi(1+2)\neq\phi(1)\cdot\phi(2)$．所以$\phi$不保持运算，$\phi$不是$\mathbf{R}$与$\mathbf{R}^+$间的一个同构映射．

注 $\psi: x\to 2^x$ 是$\mathbf{R}$与$\mathbf{R}^+$间的一个同构映射．

3) ① 正确．事实上，$\forall m,n\in\mathbf{Z}$，$\phi(m+n)=(-1)^{m+n}=(-1)^m\cdot(-1)^n=\phi(m)\cdot\phi(n)$．

② 不正确．因为 $2\in\mathbf{R}^*$ 在ϕ下没有逆象．

③ 不正确．因为 $2,4\in\mathbf{R}^*$，虽 $2\neq 4$，但$\phi(2)=1=\phi(4)$．

4) ① 正确．事实上，$\forall m,n\in\mathbf{Z}$，有$\phi(m+n)=i^{m+n}=i^m\cdot i^n=\phi(m)\cdot\phi(n)$．

② 不正确．因为 $3+4i\in\mathbf{C}^*$ 在ϕ下无逆象．

③ 不正确．因为 $4,8\in\mathbf{Z}$，虽 $4\neq 8$，但$\phi(4)=i^4=1=i^8=\phi(8)$．

5) 不正确．事实上，假设$\mathbf{C}\cong\mathbf{C}^*$，而$\phi$是$\mathbf{C}$与$\mathbf{C}^*$间的任一同构映射．对于$-1\in\mathbf{C}^*$，由$\phi$是满射，$\exists a_0\in\mathbf{C}$，使得$\phi(a_0)=-1$．由 a_0 的逆元$-a_0$ 的象是 a_0 的象-1 的逆元-1，有$\phi(-a_0)=-1$．再由ϕ是单射，有 $a_0=-a_0$，即 $2a_0=0$，从而 $a_0=0$，于是$\phi(0)=-1$．但由$\mathbf{C}$的单位元 0 的象是$\mathbf{C}^*$ 的单位元 1，有$\phi(0)=1$．而ϕ是映射，有$-1=1$，此为不可能．所以$\mathbf{C}$与$\mathbf{C}^*$不同构．

注 利用群的同态的性质较易证明．参看第二章，二，8；第二章，三，8 及第二章，四，9．

2. 证 1) ϕ显然是映射．$\forall z\in\overline{G}$，$\exists\theta\in G$，使得 $z=e^{i\theta}$，即，使$\phi(\theta)=z$，所以ϕ是满射．又 $\forall x,y\in G$，有$\phi(x+y)=e^{i(x+y)}=e^{ix}\cdot e^{iy}=\phi(x)\cdot\phi(y)$．所以$\phi$保持运算．

2) $\forall\alpha\in G$，都有 $\alpha=2^n\alpha_1$，其中 $\alpha_1(\in G)$的分子和分母均与 2 互素，而 n 是整数，所以 $\exists n\in\overline{G}$，使得$\phi(\alpha)=n$，又 $\forall\alpha,\alpha'\in G$，有 $\alpha=2^n\alpha_1$，$\alpha'=2^{n'}\alpha_1'$，其中 α_1,α_1'的分子和分母均与 2 互素，而 $n,n'\in\overline{G}$．若 $\alpha=\alpha'$，则 $2^n\alpha_1=2^{n'}\alpha_1'$，于是$\dfrac{\alpha_1'}{\alpha_1}=\dfrac{2^n}{2^{n'}}=2^{n-n'}$．因 α_1,α_1'的分子和分母均与 2 互素，故只能 $n-n'=0$，从而 $n=n'$，即$\phi(\alpha)=\phi(\alpha')$．所以$\phi$是映射．$\forall n\in\overline{G}$，$\exists\alpha=2^n\in G$，使得$\phi(\alpha)=\phi(2^n)=n$，所以$\phi$是满射．$\forall\alpha,\alpha'\in G$，有 $\alpha=2^n\alpha_1$，$\alpha'=2^{n'}\alpha_1'$，其中 α_1,α_1'的分子和分母均与 2 互素，而 $n,n'\in\overline{G}$．

$$\phi(\alpha\alpha')=\phi(2^n\alpha_1 2^{n'}\alpha_1')=\phi(2^{n+n'}\alpha_1\alpha_1')=n+n'=\phi(\alpha)+\phi(\alpha'),$$

其中 $\alpha_1\alpha_1'$的分子和分母均与 2 互素．所以ϕ是同态满射．

3) $\forall x\in G$，$\exists|\,|x|\in\overline{G}$，使得$\phi(x)=|x|$，从而$\phi$是映射．$\forall y\in\overline{G}$，$\exists y\in G$，因 $y>0$，故$\phi(y)=|y|=y$，从而ϕ是满射．$\forall x_1,x_2\in G$，

$$\phi(x_1x_2)=|x_1x_2|=|x_1||x_2|=\phi(x_1)\phi(x_2),$$

从而ϕ是同态满射．

注 由上面的 2)与 3)，依同态的传递性(第二章，二，5)，有非零有理数乘群与整数加群同态．

3. 证 1)显然．

2） 易证.

3） 自证．参看第二章，二，1.

4） 显然ϕ是G与$\overline{G}$间的一个一一映射．$\forall a+b\sqrt{2}, c+d\sqrt{2}\in G$，

$$\phi((a+b\sqrt{2})(c+d\sqrt{2}))=\phi(ac+2bd+(ad+bc)\sqrt{2})=\begin{pmatrix}ac+2bd & 2(ad+bc)\\ ad+bc & ac+2bd\end{pmatrix}$$

$$=\begin{pmatrix}a & 2b\\ b & a\end{pmatrix}\begin{pmatrix}c & 2d\\ d & c\end{pmatrix}=\phi(a+b\sqrt{2})\phi(c+d\sqrt{2}).$$

所以ϕ是G与$\overline{G}$间的一个同构映射.

5） 易证.

6） 显然ϕ是G与$\overline{G}$间的一个一一映射．$\forall \cos\theta_1+\mathrm{i}\sin\theta_1, \cos\theta_2+\mathrm{i}\sin\theta_2\in G$，

$$\phi((\cos\theta_1+i\sin\theta_1)(\cos\theta_2+i\sin\theta_2))=\phi(\cos(\theta_1+\theta_2)+\mathrm{i}\sin(\theta_1+\theta_2))$$

$$=\begin{pmatrix}\cos(\theta_1+\theta_2) & -\sin(\theta_1+\theta_2)\\ \sin(\theta_1+\theta_2) & \cos(\theta_1+\theta_2)\end{pmatrix}=\begin{pmatrix}\cos\theta_1\cos\theta_2-\sin\theta_1\sin\theta_2 & -(\cos\theta_1\sin\theta_2+\sin\theta_1\cos\theta_2)\\ \cos\theta_1\sin\theta_2+\sin\theta_1\cos\theta_2 & \cos\theta_1\cos\theta_2-\sin\theta_1\sin\theta_2\end{pmatrix}$$

$$=\begin{pmatrix}\cos\theta_1 & -\sin\theta_1\\ \sin\theta_1 & \cos\theta_1\end{pmatrix}\begin{pmatrix}\cos\theta_2 & -\sin\theta_2\\ \sin\theta_2 & \cos\theta_2\end{pmatrix}=\phi(\cos\theta_1+\mathrm{i}\sin\theta_1)\phi(\cos\theta_2+\mathrm{i}\sin\theta_2).$$

所以ϕ是G与$\overline{G}$间的一个同构映射.

7） 自证.

8） 自证.

9） $\forall p\in G$，

$$(C^{-1}PC)'B(C^{-1}PC)=C'P'(C^{-1})'BC^{-1}PC=C'P'APC=C'AC=B.$$

因此，$\exists\ C^{-1}PC\in\overline{G}$，使得$\phi(P)=C^{-1}PC$．所以$\phi$是映射．$\forall Q\in\overline{G}$，

$$(CQC^{-1})'A(CQC^{-1})=(C^{-1})'Q'C'ACQC^{-1}=(C^{-1})'Q'BQC^{-1}=(C^{-1})'BC^{-1}=A.$$

因此，$\exists CQC^{-1}\in G$，使得$\phi(CQC^{-1})=Q$．所以ϕ是满射．$\forall P_1, P_2\in G$，若$C^{-1}P_1C=C^{-1}P_2C$，则$P_1=P_2$．所以ϕ是单射．若$P_1, P_2\in G$，则

$$\phi(P_1P_2)=C^{-1}(P_1P_2)C=(C^{-1}P_1C)(C^{-1}P_2C)=\phi(P_1)\phi(P_2).$$

所以ϕ是G与$\overline{G}$间的一个同构映射.

10） 自证．该题说明无限群可能和它的真子群同构.

4. 解 设ϕ是从$\mathbb{Z}$到$\mathbb{Q}$的任意一个同态满射，则$\forall n\in\mathbb{Z}$，$\phi(n)=\phi(n\cdot 1)=n\cdot\phi(1)$，其中$\phi(1)$是$\mathbb{Q}$中任意一个数$c$．因此，从$\mathbb{Z}$到$\mathbb{Q}$的所有的同态是$\phi: n\to cn, c\in\mathbb{Q}$.

5. 解 设ϕ是$\mathbb{Z}$的任意一个自同态．当n是任意正整数时，

$$\phi(n)=\phi(\overbrace{1+1+\cdots+1}^{n\text{个}})=\overbrace{\phi(1)+\phi(1)+\cdots+\phi(1)}^{n\text{个}}=n\phi(1),$$

$$\phi(-n)=\phi(\overbrace{-1-1-\cdots-1}^{n\text{个}})=\overbrace{\phi(-1)+\phi(-1)+\cdots+\phi(-1)}^{n\text{个}}$$

$$=\overbrace{-\phi(1)-\phi(1)-\cdots-\phi(1)}^{n\text{个}}=-n\phi(1),$$

$$\phi(0)=0=0\phi(1).$$

因此，$\mathbb{Z}$的自同态应形如：$\forall a\in\mathbb{Z}$，$\phi: a\to ak$，其中$k=\phi(1)$是一个固定的整数.

反之，$\forall a\in\mathbb{Z}$，$\phi: a\to ak$，其中k是任意一个整数，显然都是$\mathbb{Z}$的自同态.

所以，$\mathbb{Z}$ 的所有自同态为$\phi:a\to ak$，其中 k 是任意整数．从而 $\mathbb{Z}$ 的自同态有无穷多个.

当 $k\neq 1$ 且 $k\neq -1$ 时，若 $ak=1$，则 $a=\frac{1}{p}\overline{\in}\mathbb{Z}$，说明 1 在$\phi$下无逆象，即$\phi:a\to ak$ 不是满射．所以 $\mathbb{Z}$ 的自同构只有两个：恒等变换$\phi_1:a\to a(k=1)$和反号变换$\phi_2:a\to -a(k=-1)$.

6. 证 （反证法）若 G 不是交换群，则 $\exists a,b\in G$，使得 $ab\neq ba$，即 $aba^{-1}\neq b$. 从而，虽 $x\to axa^{-1}$是 G 的自同构，但不是恒等变换，此与已知矛盾．所以 G 是交换群．若 $\exists a\in G$，而 $a^2\neq e$，即 $a\neq a^{-1}$，则虽 $x\to x^{-1}$是 G 的自同构，但不是恒等变换，此与已知矛盾．所以，$\forall x\in G$，都有 $x^2=e$.

7. 自证.

8. 证 设

$$G=\{\tau\mid \tau \text{ 是 } A \text{ 的一一变换，且 } a^{\tau}=a\}.$$

因 A 的恒等变换 $\varepsilon\in G$，故 $G\neq\varnothing$. $\forall \tau,\sigma\in G$，$a^{\tau\sigma}=(a^{\tau})^{\sigma}=a^{\sigma}=a$，从而 $\tau\sigma\in G$. 变换乘法适合结合律．G 有单位元 ε. $\forall\tau\in G$，因 τ 是一一变换，又 $a^{\tau}=a$，故 $\exists\tau$ 的逆变换 τ^{-1}，使得 $a^{\tau^{-1}}=a$，从而 $\tau^{-1}\in G$. 且 $\forall b\in A$，设 $b^{\tau}=c$，则 $c^{\tau^{-1}}=b$，于是 $b^{\tau\tau^{-1}}=(b^{\tau})^{\tau^{-1}}=c^{\tau^{-1}}=b$，从而 $\tau\tau^{-1}=\varepsilon$，即 τ 有右逆元 $\tau^{-1}\in G$. 因此 G 是群．又 G 中元都是 A 的一一变换，所以 G 是 A 的变换群.

9. 证 1) G 的运算表是

	τ_1	τ_2	τ_3
τ_1	τ_1	τ_2	τ_3
τ_2	τ_2	τ_3	τ_1
τ_3	τ_3	τ_1	τ_2

τ_1 是 G 的单位元，τ_1,τ_2,τ_3 的逆元分别是 τ_1,τ_3,τ_2.

2) G 的运算表是

	τ_1	τ_2
τ_1	τ_1	τ_2
τ_2	τ_2	τ_1

τ_1 是 G 的单位元．τ_1,τ_2 的逆元分别都是自身.

10. 证 1) 因 $\tau_{I,0}\in G$，故 $G\neq\varnothing$. 又显然 $\forall\tau_{A,B}(\in G)$都是 $M_n(\mathbf{R})$的一一变换．$\forall\tau_{A,B},\tau_{C,D}\in G$，$\forall X\in M_n(\mathbf{R})$，$X^{\tau_{A,B}\tau_{C,D}}=(X^{\tau_{A,B}})^{\tau_{C,D}}=(AX+B)^{\tau_{C,D}}=C(AX+B)+D=(CA)X+(CB+D)=X^{\tau_{CA,CB+D}}$，从而 $\tau_{A,B}\tau_{C,D}=\tau_{CA,CB+D}$. 因 $|C|\neq 0$，$|A|\neq 0$，故 $|CA|=|C||A|\neq 0$，且 $CA,CB+D\in M_n(\mathbf{R})$，从而 $\tau_{A,B}\tau_{C,D}\in G$. $\exists\tau_{I,0}\in G$，使得 $\forall\tau_{A,B}\in G$，$\tau_{A,B}\tau_{I,0}=\tau_{IA,IB+0}=\tau_{A,B}$. $\forall\tau_{A,B}\in G$，$\exists\tau_{A,B}{}^{-1}=\tau_{A^{-1},-A^{-1}B}\in G$，使得 $\tau_{A,B}\tau_{A^{-1},-A^{-1}B}=\tau_{A^{-1}A,A^{-1}B-A^{-1}B}=\tau_{I,0}$. 所以 G 是 $M_n(\mathbf{R})$的一个变换群.

2)—6) 自证.

11. 解 1) $\{\tau_m\mid\tau_m:n\to n+m,m\in\mathbb{Z}\}$.

2) $\left\{\tau_x \middle| \tau_x: r \to r+x, x \in \mathbb{R}\right\}$.

3) $\left\{\tau_x \middle| \tau_x: r \to rx, x \in \mathbb{R}^*\right\}$.

4) $\left\{\tau_A \middle| \tau_A: X \to X+A, A \in M_n(\mathbb{R})\right\}$.

5) $\left\{\tau_A \middle| \tau_A: X \to XA, A \in GL_n(\mathbb{R})\right\}$.

6) $\left\{\tau_a \middle| \tau_a: x \to x+a, a \in \mathbb{Q}\right\}$.

7) $\left\{\tau_a \middle| \tau_a: x \to xa, a \in \mathbb{Q}^*\right\}$.

8) $\left\{\tau_{(a,b)} \middle| \tau_{(a,b)}: (x,y) \to (x+a, y+b), (a,b) \in \pi\right\}$.

注 1) $H=\{\tau_{(a,0)} \mid \tau_{(a,0)}: (x,y) \to (x+a, y), (a,0) \in \pi\}$也是$\pi$的一个变换群,但不与$\pi$同构.

2) $\forall a \in \mathbb{R}, \tau_a: (x,y) \to (x+a, 0)$是$\pi$的变换,但不是$\pi$的一一变换. 令$G=\{\tau_a \mid a \in \mathbb{R}\}$. 则$G$对于变换乘法作成一个群. 事实上,$\forall \tau_a, \tau_b \in G, \forall (x,y) \in \pi, (x,y)^{\tau_a \tau_b}=\left((x,y)^{\tau_a}\right)^{\tau_b}=(x+a,0)^{\tau_b}=(x+a+b,0)=(x,y)^{\tau_{a+b}}$,从而$\tau_a\tau_b=\tau_{a+b} \in G$. $\exists \tau_0 \in G$,使得$\tau_0\tau_a=\tau_a\tau_0=\tau_a, \forall \tau_a \in G$. 又$\forall \tau_a \in G, \exists \tau_a^{-1}=\tau_{-a} \in G$,使得$\tau_{-a}\tau_a=\tau_a\tau_{-a}=\tau_0$,且变换乘法适合结合律. 所以$G$是一个群. 但$G$不是$\pi$的变换群.

3) 设$\phi: \tau_{(a,0)} \to a$,则$H \overset{\phi}{\cong} \mathbb{R}$.

4) 设$\psi: a \to \tau_a$,则$\mathbb{R} \overset{\psi}{\cong} G$.

5) 设$\bar{\pi}=\left\{(x,y) \middle| x \neq 0, x,y \in \mathbb{R}\right\}$. 规定$(x,y)=(x',y')$当且仅当$x=x', y=y'$. 则$\bar{\pi}$对于代数运算

$$(x,y)(x',y')=(x'x, x'y+y')$$

来说作成一个群. $\forall (a,b) \in \bar{\pi}$,

$$\tau_{(a,b)}: (x,y) \to (ax, ay+b)=(x,y)(a,b)$$

是$\bar{\pi}$的一个一一变换. 作$K=\left\{\tau_{(a,b)} \middle| \tau_{(a,b)}: (x,y) \to (ax, ay+b), (a,b) \in \bar{\pi}\right\}$,则由 Cayley 定理,$\bar{\pi} \cong K$,其中$K$是$\bar{\pi}$的变换群.

第六章

1. 解 1) $(1\ 2\ 4\ 6\ 5\ 7)^{-2}=[(1\ 2\ 4\ 6\ 5\ 7)(1\ 2\ 4\ 6\ 5\ 7)]^{-1}=[(1\ 4\ 5)(2\ 6\ 7)]^{-1}=(2\ 6\ 7)^{-1}(1\ 4\ 5)^{-1}=(7\ 6\ 2)(5\ 4\ 1)$.

2) $x=(1\ 2\ 4)^{-1}(3\ 4\ 6)(1\ 5)=(4\ 2\ 1)(3\ 4\ 6)(1\ 5)=(4\ 2\ 5\ 1\ 6\ 3)$.

3) $x=(ij)^{-1}(ik)=(ij)(ik)=(ijk)$.

2. 解 不成立. 例,取$(1\ 2),(1\ 3),(2\ 3) \in S_3$,虽$|(1\ 2)|=|(1\ 3)|=2, |(1\ 2)|=|(2\ 3)|=2$,但$(1\ 2)(1\ 2)=(1), (1\ 3)(2\ 3)=(1\ 2\ 3)$,因此$|(1\ 2)(1\ 2)|=1 \neq 3=|(1\ 3)(2\ 3)|$.

3. 证 $\phi: (1) \to 1, (1\ 2\ 3) \to 1, (1\ 3\ 2) \to 1, (1\ 2) \to -1, (1\ 3) \to -1, (2\ 3) \to -1$是$S_3$到$H$的一个同态满射.

4. 解 设$\pi \in S_p$,π的阶为p. 则π可分解成不相连的循环置换的乘积,且p为π的这

些循环置换因子的长的最小公倍数．因 p 是素数，故 p 只能是 1 与 p 的最小公倍数．因此 π 只能是 p－循环置换．而 S_p 内的 p－循环置换共有 $\frac{p!}{p}=(p-1)!$ 个，所以 S_p 内共有 $(p-1)!$ 个 p 阶元.

5. 解 1) 不对．如整数加群 $\mathbb{Z}$ 只能由 ± 1 生成，其他的元都不是 $\mathbb{Z}$ 的生成元.

2) 对.

3) 对.

4) 对.

5) 不对．如模 4 的剩余类加群 $\mathbb{Z}_4$ 的阶是 $4=2^n$，这里 2 不是奇数.

6) 不对．如有理数集 $\mathbb{Q}$ 对于普通加法作成一个群．$2(\in\mathbb{Q})$ 的阶无限，但 $\mathbb{Q}$ 与整数加群 $\mathbb{Z}$ 不同构，因此 $\mathbb{Q}$ 不是循环群（见第二章，四，9，1)）.

7) 不对．如由 $(1\ 2\ 3)(1\ 2)$ 生成的循环群是交换群，但 $(1\ 2\ 3)(1\ 2)=(2\ 3)\neq(1\ 3)=(1\ 2)(1\ 2\ 3)$.

8) 对．设 $G=\left\{\begin{pmatrix}1 & 0\\ n & 1\end{pmatrix}\middle| n \text{ 是整数}\right\}$，则

$$\phi: n\to\begin{pmatrix}1 & 0\\ n & 1\end{pmatrix}.$$

显然是整数加群 $\mathbb{Z}$ 与 G 间的一个一一映射．又 $\forall n,m\in\mathbb{Z}$，

$$\phi: n\to\begin{pmatrix}1 & 0\\ n & 1\end{pmatrix}, m\to\begin{pmatrix}1 & 0\\ m & 1\end{pmatrix}.$$

因此

$$\phi: n+m\to\begin{pmatrix}1 & 0\\ n+m & 1\end{pmatrix}=\begin{pmatrix}1 & 0\\ n & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ m & 1\end{pmatrix}.$$

所以 $\mathbb{Z}\overset{\phi}{\cong}G$. 因 $\mathbb{Z}$ 是循环群，故 G 也是循环群.

实际上，$\exists\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\in G$，使得 $\forall\begin{pmatrix}1 & 0\\ n & 1\end{pmatrix}\in G$，都有 $\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}^n=\begin{pmatrix}1 & 0\\ n & 1\end{pmatrix}$，而 $\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}^0=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$（$G$ 的单位元），从而 $G=\left(\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\right)$.

9) 不对．因循环群必为交换群，但 S_3 不是交换群，故 S_3 不是循环群.

10) 对．$G=(2)$.

11) 对．$G=([2])$.

12) 不对．设 $\mathbb{Z}_{12}$ 是模 12 的剩余类加群，$[1],[5]\in\mathbb{Z}_{12}$，虽 $12[1]=12[5]=[0]$，但 $[1]\neq[5]$.

6. 证 1) 因 G_2 有且只有两个生成元 b 与 b^{-1}，而在同构映射下，生成元映到生成元，故 G_1 与 G_2 间的同构映射有且只有两个：

$$\phi_1: a\to b,\ \text{即}\ a^h\to b^h,$$
$$\phi_2: a\to b^{-1},\ \text{即}\ a^h\to(b^{-1})^h.$$

2) 因 G_2 有且只有 $\varphi(n)$ 个生成元：b^r．$(r,n)=1$．而在同构映射下，生成元映到生成

元，故 G_1 与 G_2 间的同构映射有且只有 $\psi(n)$个：

$$\psi:\ a\to b^r,\ (r,n)=1,$$

即

$$\psi:\ a^h\to(b^r)^h,\ (r,n)=1.$$

注 由此命题得知，无限循环群的自同构有且只有两个，而 n 阶循环群的自同构有且只有 $\psi(n)$个.

7. 解 $\mathbb{Z}_6=([1])=\{[0],[1],[2],[3],[4],[5]\}$. $[0],[1],[2],[3],[4],[5]$的阶分别是$\frac{6}{(0,6)}=1,\frac{6}{(1,6)}=6,\frac{6}{(2,6)}=3,\frac{6}{(3,6)}=2,\frac{6}{(4,6)}=3,\frac{6}{(5,6)}=6$. 因$(1,6)=(5,6)=1$，即小于6且与6互素的正整数有且只有两个：1与5，故$[1]$与$5[1]=[5]$是$\mathbb{Z}_6$的全部生成元.

注 设 $a,b\in$群G，虽$|a|\neq2,|b|\neq2$，且 $a\neq b^{-1}$，但可能$|ab|=2$. 例，$[1],[2]\in\mathbb{Z}_6$，$\big|[1]\big|=6\neq2,\big|[2]\big|=3\neq2$，且$[1]\neq[4]=-[2]$，但$\big|[1]+[2]\big|=\big|[3]\big|=2$.

8. 证一 $(\Rightarrow)$ $\forall a^n\in(a)$，

$$\phi:\ a^n\to b^{nk}$$

是(a)到(b)的一个同态映射．事实上，

1） ϕ是(a)到(b)的一个映射．$\forall a^n\in(a)$，$\exists b^{nk}\in(b)$，使得$\phi:a^n\to b^{nk}$. 且这样的 b^{nk}唯一．因为，$a^n=a^m\Rightarrow a^{n-m}=e\overset{|a|=s}{\Longrightarrow}s\,\big|\,n-m\Rightarrow\exists q\in\mathbb{Z}$，使得 $n-m=sq\Rightarrow b^{nk-mk}=b^{(n-m)k}=sqk$. 由已知 $t\,\big|\,sk$，从而 $sk=tu,u\in\mathbb{Z}$. 所以

$$b^{nk-mk}=b^{(sk)q}=b^{(tu)q}=(b^t)^{uq}\xlongequal{\text{由 }|b|=t}e'^{uq}=e'.$$

因此 $b^{nk}=b^{mk}$.

2） ϕ保持运算．$\forall a^n,a^m\in(a)$，

$$\phi:\ a^n\to b^{nk},\ a^m\to b^{mk}.$$

从而

$$\phi:\ a^na^m=a^{n+m}\to b^{(n+m)k}=b^{nk}b^{mk}.$$

所以ϕ是(a)到(b)的一个同态映射.

显然，取 $n=1$ 时，$\phi:a\to b^k$；取 $n=0$ 时，$\phi:e\to e'$，其中 e,e'分别是(a)，(b)的单位元.

$(\Leftarrow)$ 若存在一个(a)到(b)的同态映射ϕ，使

$$\phi:\ a\to b^k,\ e\to e',$$

其中 e,e'分别是(a)，(b)的单位元．因ϕ是同态映射，故

$$\phi:\ a^s=\overbrace{aa\cdots a}^{s\text{个}}\to\overbrace{b^k\,b^k\,\cdots\,b^k}^{s\text{个}}=(b^k)^s=b^{sk}.$$

又 $a^s=e$，ϕ是(a)到(b)的映射，从而 $b^{sk}=e'$，令$|b|=t$，所以 $t\,\big|\,sk$.

证二 $(\Rightarrow)$ $\forall a^n\in(a),0\leqslant n<s$，

$$\phi:\ a^n\to b^{nk}$$

是(a)到(b)的同态映射．事实上，

1） $\forall a^n\in(a)$，$\exists b^{nk}\in(b)$，使得$\phi(a^n)=b^{nk}$. 且这样的 b^{nk}唯一．因为，若 $a^n=a^m$，$0\leqslant n,m<s$，则 $a^{n-m}=e,0\leqslant n-m<s$. 因$|a|=s$，故 $s\,\big|\,n-m$，但 $0\leqslant n-m<s$，从而 $n-m=0$，即 $n=m$，所以，$b^{nk}=b^{mk}$，因此ϕ是(a)到(b)的一个映射.

2) $\forall a^n, a^m \in (a), \phi(a^n)=b^{nk}, \phi(a^m)=b^{mk}$. 设 $n+m=qs+r, 0\leqslant r<s$, 则 $\phi(a^na^m)=\phi(a^{n+m})=\phi(a^{qs+r})\xlongequal{\text{由}|a|=s}\phi(a^r)=b^{rk}=b^{(n+m)k-qsk}$. 因 $t \mid sk$, 故 $\exists q'\in \mathbb{Z}$, 使得 $sk=q't$. 所以 $\phi(a^na^m)=b^{(n+m)k-qq't}=b^{nk}b^{mk}(b^t)^{-qq'}\xlongequal{\text{由}|b|=t}b^{nk}b^{mk}=\phi(a^n)\phi(a^m)$.

所以ϕ是(a)到(b)的一个同态映射.

其余部分的证明与证一相同.

第七章

1. 略.

2. 证 设 $G=(a)=\{a^0=e, a, a^2, \cdots, a^{n-1}\}$是 n 阶循环群. 因 $t \mid n$, 故 G 有唯一的一个 t 阶循环子群 $H=(a^s)=\{(a^s)^0=e, a^s, (a^s)^2, \cdots, (a^s)^{t-1}\}$.

1) 设

$$\begin{aligned} H_1 &= \{x^s \mid x\in G\} \\ &= \{e^s, a^s, (a^2)^s, \cdots, (a^{n-1})^s\} \\ &= \{e, a^s, (a^s)^2, \cdots, (a^s)^{n-1}\}. \end{aligned}$$

下面证明 $H_1=H$. 显然 $H\subset H_1$. 另一方面, $\forall (a^s)^m\in H_1$, $\exists q, r\in\mathbb{Z}$, 使得 $m=tq+r, 0\leqslant r<t$.

$$(a^s)^m=(a^s)^{tq+r}=(a^{st})^q(a^s)^r=(a^n)^q(a^s)^r=e^q(a^s)^r=(a^s)^r\in H,$$

从而 $H_1\subset H$. 所以 $H_1=H$.

2) 设

$$H_2=\{h\in G \mid h^t=e\}.$$

下面证明 $H_2=H$. $\forall (a^s)^i\in H$, 有 $((a^s)^i)^t=e$, 于是$(a^s)^i\in H_2$, 从而 $H\subset H_2$. 另一方面, $\forall h=a^j\in H_2$, $a^{jt}=(a^j)^t=e$, 因$|a|=n$, 故 $n\mid jt$, 即$\exists l\in\mathbb{Z}$, 使得 $jt=ln=lst$. 因 $t\neq 0$, 故 $j=ls$, 于是

$$h=a^j=a^{ls}=(a^s)^l\in H_1=H,$$

从而 $H_2\subset H$, 所以 $H_2=H$.

3. 解 1) $|[25]|=6$, $([25])=\{0[25], [25], 2[25], 3[25], 4[25], 5[25]\}=\{[0], [25], [20], [15], [10], [5]\}$.

2) 因$(2,3)=1$, 故$\exists s, t\in\mathbb{Z}$, 使得 $2s+3t=1$, 从而 $1\in(S)$. $\forall n\in\mathbb{Z}$, $n=n1\in(S)$, 所以$(S)=\mathbb{Z}$.

3) $(S)=\mathbb{Q}^+$.

4) $(S)=$有理数集对加法作成的群$\mathbb{Q}$. 因$\forall \dfrac{n}{m}\in\mathbb{Q}$. 当 $n>0$ 时, 有

$$\frac{n}{m}=\overbrace{\frac{1}{m}+\frac{1}{m}+\cdots+\frac{1}{m}}^{n\text{个}}.$$

当 $n<0$ 时, 有

$$\frac{n}{m}=\overbrace{-\frac{1}{m}+\left(-\frac{1}{m}\right)+\cdots+\left(-\frac{1}{m}\right)}^{n\text{个}}.$$

当 $n=0$ 时，有

$$\frac{n}{m}=1+(-1).$$

所以$\frac{n}{m}\in(S)$，从而$(S)=\mathbb{Q}$.

5) 因 $ab=\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}=c,a^2=b^2=c^2=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=e,ac=b,ba=c,bc=a,ca=b,cb=a$，故 $H=\{e,a,b,c\}$有乘法表

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

且 H 是包含 a,b 的最小子群．所以$(S)=$Klein 四元群 H.

6) $(S)=GL_n(\mathbb{R})$.

7) $(S)=(H\cup K)=M_n(\mathbb{R})$.

4. 证 首先确定 $H=(S)$中元的形状．因 $ab=ba,a^2=e,b^3=e$，即 $a^{-1}=a,b^{-1}=b^2$，故 H 中元的形状为 $a^mb^n,m=0,1;n=0,1,2$. 共有 6 种取法，从而 $H=(S)$为 6 阶群.

因 $ab=ba,|a|=2,|b|=3$，而$(2,3)=1$，故由第七章，二，8，$|ab|=2\times3=6$. 所以 $H=(ab)$是 6 阶循环群．其中 6 个元是：

$$a^0b^0=e=(ab)^0,a^0b=b=(ab)^4,a^0b^2=b^2=(ab)^2,$$
$$ab^0=a=(ab)^3,ab,ab^2=(ab)^5.$$

注 该命题可推广为：设 $a,b\in$群 G，且$|a|=m,|b|=n,(m,n)=1,ab=ba$，则由集 $S=\{a,b\}$生成的子群 $H=(S)$是 mn 阶循环群(ab).

5. 解 只需取 $H'=\{(a,b)\mid a,b\in\mathbb{Q}\}$.

6. 解 都不正确．证法一中未解决 e 是否在 H 中．证法二中，由 $a\in H$ 得 $e'a=a$，说明不了 e'是 G 的单位元.

7. 证 因 G 是有限群，故 $a\in G$，$|a|$有限，设$|a|=n$，于是 $a^n=e\in H$. 因此 $n\in$集$\{s\mid s$ 是正整数$,a^s\in H\}\neq\varnothing$，所以该集有最小正整数 m，即存在最小正整数 m，使 $a^m\in H$.

下面证明 $m\mid n$. 设 $n=qm+r,0\leqslant r<m$，则

$$a^r=a^{n-qm}=a^n(a^m)^{-q}=(a^m)^{-q}\in H.$$

由 $0\leqslant r<m$ 及 m 的最小性，有 $r=0$，所以 $m\mid n$.

8. 证 取 $a\in G$，则$(a)<G$. 若(a)是有限群，则再取 $b\in G-(a)$，$(b)<G$. 若(b)还是有限群，则再取 $c\in G-(a)-(b)$，又得(c)，$(c)<G$. 这样继续做下去．如果某子群，设为(a)，是无限群，则$(a^2)\neq(a)$，且(a^3)，(a^4)，…都是 G 的不同子群．所以无论何时 G 总有无限个不同的子群.

9. 证 1) 若 G 是循环群，则因$|G|=mn,1<m<|G|,1<n<|G|$，故由第七章，一，

10，G 有 m 阶真子群． 2)若 G 不是循环群．因 $|G|$ 是合数，故 $|G|>1$，$\exists x\in G$，$x\neq e$，则由 x 生成的循环群 (x) 是 G 的一个真子群．事实上，显然 $(x)<G$，又 $(x)\neq\{e\}$，$(x)\neq G$，不然 G 是循环群，产生矛盾．所以 (x) 是 G 的一个真子群.

10. 证 若 s,t 至少有一个为 0，结论显然成立．若 s,t 都 $\neq 0$，今证 $H\cap K=(a^d)$.

因 $d=[s,t]$，故 $\exists s_1,t_1\in\mathbb{Z}$，使得 $d=ss_1=tt_1$，且 $(s_1,t_1)=1$. 于是 $a^d=(a^s)^{s_1}=(a^t)^{t_1}\in H\cap K$，所以 $(a^d)\subset H\cap K$.

另一方面，$\forall x\in H\cap K<G=(a)$，$\exists m\in\mathbb{Z}$，使得 $x=a^m$，且 $a^m\in H=(a^s)$，$a^m\in K=(a^t)$，从而 $\exists m_1,m_2\in\mathbb{Z}$，使得 $a^m=(a^s)^{m_1}=(a^t)^{m_2}$.

1) 若 $|a|=\infty$，则 $m=sm_1=tm_2$，即 $s\mid m$，$t\mid m$，从而 $d=[s,t]\mid m$，因此 $\exists q\in\mathbb{Z}$，使得 $m=dq$，于是 $x=a^m=(a^d)^q\in(a^d)$，所以 $H\cap K\subset(a^d)$.

2) 若 $|a|=n$，则 $n\mid m-sm_1$，$n\mid m-tm_2$，即 $n\mid s_1(m-sm_1)=s_1m-dm_1$，$n\mid t_1(m-tm_2)=t_1m-dm_2$. 因 $(s_1,t_1)=1$，故 $\exists u,v\in\mathbb{Z}$，使得 $us_1+vt_1=1$. 由 $n\mid u(s_1m-dm_1)$，$n\mid v(t_1m-dm_2)$，有

$$n\mid m(us_1+vt_1)-d(um_1+vm_2)=m-d(um_1+vm_2).$$

因此 $\exists r\in\mathbb{Z}$，使得 $m-d(um_1+vm_2)=nr$，于是 $x=a^m=a^{d(um_1+vm_2)+nr}=(a^d)^{um_1+vm_2}(a^n)^r$ $\xlongequal{|a|=n}(a^d)^{um_1+vm_2}\in(a^d)$，所以 $H\cap K\subset(a^d)$.

综上，$H\cap K=(a^d)$.

注 由此命题直接可知：无限循环群 $G=(a)$ 的任两个非单位子群 $H=(a^s)$ 与 $K=(a^t)$ 的交 $H\cap K$ 也是非单位子群．事实上，由该命题知 $H\cap K=(a^d)$，$d=[s,t]$. 因 $H\neq\{e\}$，$K\neq\{e\}$，故 $a\neq e$，$s\neq 0$，$t\neq 0$，从而 $d\neq 0$. 又因 G 是无限循环群，故 $a^d\neq a^0=e$. 所以 $H\cap K=(a^d)\neq\{e\}$. (还可如下证明：因 $H=(a^s)\neq\{e\}$，$K=(a^t)\neq\{e\}$，故 $a\neq e$，$s\neq 0$，$t\neq 0$，又 $|a|=\infty$，于是 $a^{st}\neq e$. 而 $a^{st}=(a^s)^t=(a^t)^s\in H\cap K$，所以 $H\cap K\neq\{e\}$.)

11. 证一 设 H 与 K 是 G 的任意两个真子群，则 $\exists a,b\in G$，使得 $a\notin H$，$b\notin K$.

1) 若 $a\notin K$，则 $a\notin H\cup K$，从而 $G\neq H\cup K$.

2) 若 $b\notin H$，则 $b\notin H\cup K$，从而 $G\neq H\cup K$.

3) 若 $a\in K$ 且 $b\in H$，则 $ab\notin H\cup K$. 事实上，假定 $ab\in H\cup K$，则 $ab\in H$ 或 $ab\in K$. 若 $ab\in H$，由 $b\in H$，H 是子群，有 $b^{-1}\in H$，于是 $a=abb^{-1}\in H$，此与 $a\notin H$ 矛盾．所以 $ab\notin H$. 同理 $ab\notin K$. 因此 $ab\notin H\cup K$. 但 $ab\in G$，从而 $G\neq H\cup K$.

证二 (反证法)假定存在 G 的两个真子群 H 与 K，使 $G=H\cup K$，则 $\exists a,b\in G$，使得 $a\notin H$，但 $a\in K$；$b\notin K$，但 $b\in H$，且 $ab\in G=H\cup K$. 因此 $ab\in H$ 或 $ab\in K$. 与证一相同，推出矛盾.

证三 (反证法)假定存在 G 的两个真子群 H 与 K，使 $G=H\cup K$，则 $\exists a,b\in G$，使得 $a\notin H$，$a\in K$，$b\notin K$，$b\in H$. 于是 $aH\cap H=\varnothing$. 事实上，若有 $x\in aH\cap H$，则 $x\in aH$ 且 $x\in H$，即 $x=ah$，$h\in H$，因 H 是子群，故 $h^{-1}\in H$，进而 $a=xh^{-1}\in H$，此与 $a\notin H$ 矛盾．所以 $aH\cap H=\varnothing$. 同理 $bK\cap K=\varnothing$. 由 $G=H\cup K$，有 $aH\subset K$ 且 $bK\subset H$. 于是 $baH\subset bK\subset H$，即 $ba\in H$，可设 $ba=h$，$h\in H$，因 H 是子群，故 $a=b^{-1}h\in H$，此与 $a\notin H$ 矛盾.

证四 (反证法)假定存在 G 的两个真子群 H 与 K，使 $G=H\cup K$，则 $\exists a\in G$，使得 $a\notin H$，但 $a\in K$. 由证三知 $aH\cap H=\varnothing$，进而 $aH\subset K$. $\forall x\in H$，有 $ax\in aH\subset K$，由 K 是子群，$a^{-1}\in K$，有 $x=a^{-1}(ax)\in K$，从而 $H\subset K$. 由 $G=H\cup K$，$G=K$，此与 K 是 G 的真子群矛盾.

12. 证 因 $a_ia_j=a_ja_i$，故

$$(S)=\left\{a_1^{m_1}a_2^{m_2}\cdots a_k^{m_k}\ \middle|\ m_1,m_2,\cdots,m_k\in\mathbb{Z}\right\}.$$

显然(S)是交换群．因 $|a_i|=n_i$，故 $0\leqslant m_i<n_i$，即 $a_i^{m_i}$ 的取法有 n_i 种，$i=1,2,\cdots,k$，从而(S)中元的个数 $\leqslant n_1n_2\cdots n_k$. 所以(S)是有限群.

13. 解 1) 因 $[G:H]=\dfrac{|G|}{|H|}=\dfrac{6}{2}=3$，故 H 的右陪集共有 3 个．即：$H\varepsilon_0=H\varepsilon_3=H=\{\varepsilon_0,\varepsilon_3\}$，$H\varepsilon_1=H\varepsilon_4=\{\varepsilon_1,\varepsilon_4\}$，$H\varepsilon_2=H\varepsilon_5=\{\varepsilon_2,\varepsilon_5\}$.

2) 因 $[G:H]=\dfrac{|G|}{|H|}=\dfrac{12}{3}=4$，故 H 的右陪集共有 4 个．即：$H=\{e,a^4,a^8\}$，$Ha=\{a,a^5,a^9\}$，$Ha^2=\{a^2,a^6,a^{10}\}$，$Ha^3=\{a^3,a^7,a^{11}\}$.

3) H 的右陪集是

$$\begin{aligned}H+0&=\{\cdots,-12,-8,-4,0,4,8,12,\cdots\},\\H+1&=\{\cdots,-11,-7,-3,1,5,9,13,\cdots\},\\H+2&=\{\cdots,-10,-6,-2,2,6,10,14,\cdots\},\\H+3&=\{\cdots,-9,-5,-1,3,7,11,15,\cdots\}.\end{aligned}$$

即为模 4 的剩余类：[0]，[1]，[2]，[3].

4) $\forall a\in G$，包含 a 的右陪集为 $Ha=\{a,-a\}$. 当 a,b 是不同的正有理数时，$a\neq b$ 且 $a\neq -b$，从而 $Ha=\{a,-a\}\neq Hb=\{b,-b\}$. 当 a 是负有理数时，$Ha=\{a,-a\}=H(-a)$，其中 $-a$ 是正有理数．所以 H 的所有右陪集是 $\{a,-a\}$，这里 a 是任意正有理数.

5) $\forall a\in G$，包含 a 的右陪集为 Ha. 当 a 是正有理数时，$Ha=H$；当 a 是负有理数时，$Ha=H(-a)(-1)=H(-1)=$ 负有理数集．因此 H 有且仅有两个右陪集：H 和 $H(-1)$.

14. 证 1) 显然 $H_1\cap H_2<G$. 下面证明，$\forall x\in G$，$(H_1\cap H_2)x=H_1x\cap H_2x$. $\forall hx\in(H_1\cap H_2)x$，因 $h\in H_1\cap H_2$，故 $h\in H_1$ 且 $h\in H_2$，于是 $hx\in H_1x$ 且 $hx\in H_2x$，从而 $hx\in H_1x\cap H_2x$. 所以 $(H_1\cap H_2)x\subset H_1x\cap H_2x$. 另一方面，$\forall a\in H_1x\cap H_2x$，有 $a\in H_1x$ 且 $a\in H_2x$，即 a 可表为 $a=h_1x=h_2x$，$h_1\in H_1$，$h_2\in H_2$. 由消去律得 $h_1=h_2$，记为 $h=h_1=h_2$，于是 $a=hx$. 因 $h\in H_1\cap H_2$，故 $a=hx\in(H_1\cap H_2)x$，所以 $H_1x\cap H_2x\subset(H_1\cap H_2)x$. 综上，$(H_1\cap H_2)x=H_1x\cap H_2x$. 同理，结论对左陪集也成立．

2) 因 H_1 与 H_2 在 G 里有有限指数，即 H_1 与 H_2 在 G 里不同右陪集的个数是有限的，再由前面 1)知，$H_1\cap H_2$ 在 G 里的任一右陪集都是 H_1 的一个右陪集与 H_2 的一个右陪集的交，故 $H_1\cap H_2$ 在 G 里不同右陪集的个数也是有限的．所以 $H_1\cap H_2$ 在 G 里的指数是有限的.

15. 证 只需证明 G 有 3 阶元．G 中非单位元的元的阶不能都是 2，不然，集 $\{e,a,b,ab\}$ 就是 G 的一个 4 阶子群，但 $4\nmid 6$，此与 Lagrange 定理矛盾．从而 G 中必有阶不是 2 的元 g. 于是 $|g|$ 只能是 3 或 6[①]. 若 $|g|=3$，则 $H=(g)$ 就是 G 的一个 3 阶子群．若 $|g|=6$，则 $|g^2|=\dfrac{6}{(6,2)}=3$，从而 $K=(g^2)$ 就是 G 的一个 3 阶子群.

16. 证 (反证法)若有 $x\in(a)\cap(b)$，但 $x\neq e$，则 $x\in(a)$ 且 $x\in(b)$. 于是 $|x|\,\big|\,|(a)|=|a|=p$[②]. 因 p 是素数，故 $|x|=1$ 或 p，但 $x\neq e$，从而 $|x|=p$. 又 $|(a)|=p$，于是 $(x)=(a)$.

---

①② 张禾瑞．近世代数基础．北京：高等教育出版社，1978. 69. 定理 3.

由 $x\in(b)$，$(x)\subset(b)$，即$(a)\subset(b)$，所以 $a\in(b)$，此与 $a\overline{\in}(b)$矛盾．因此$\forall x\in(a)\cap(b)$，都有 $x=e$. 即$(a)\cap(b)=\{e\}$.

17. 证一 由第七章，四，1，11)知，$G_{(k)}<G$，$G^{(k)}<G$. 已知$[G:G_{(k)}]$为有限数，可设$[G:G_{(k)}]=n$. G有右陪集分解：

$$G=G_{(k)}g_1\cup G_{(k)}g_2\cup\cdots\cup G_{(k)}g_n,$$

其中 $g_1,g_2,\cdots,g_n$ 是G中n个互不相同的元．$\forall x,y\in G$，有

$$G_{(k)}x=G_{(k)}y\Leftrightarrow xy^{-1}\in G_{(k)}\Leftrightarrow(xy^{-1})^k=e$$

$$\xLeftrightarrow{G\text{是交换群}}x^ky^{-k}=e\Leftrightarrow x^k=y^k,$$

即

$$G_{(k)}x\neq G_{(k)}y\Leftrightarrow x^k\neq y^k.$$

由 $G_{(k)}g_i\neq G_{(k)}g_j(i\neq j)\Rightarrow g_i^k\neq g_j^k$，又 $G_{(k)}$有n个不同的右陪集，$g_i^k,g_j^k\in G^{(k)}$知，$G^{(k)}$中至少有n个元$g_1^k,g_2^k,\cdots,g_n^k$.

由 $x^k\neq y^k\Rightarrow G_{(k)}x\neq G_{(k)}y$，又 $G_{(k)}$只有n个不同的右陪集，$x^k,y^k\in G^{(k)}$知，$G^{(k)}$中至多有n个元.

所以 $G^{(k)}=\{g_1^k,g_2^k,\cdots,g_n^k\}$. 即$|G^{(k)}|=n=[G:G_{(k)}]$.

证二 同证一，G有右陪集分解

$$G=G_{(k)}g_1\cup G_{(k)}g_2\cup\cdots\cup G_{(k)}g_n,$$

其中 $g_1,g_2,\cdots,g_n$ 是G中n个互不相同的元．我们建立法则：$\forall x^k\in G^{(k)}$，$x\in G$，若 $x\in G_{(k)}g_i$，$1\leqslant i\leqslant n$，则令

$$\phi:x^k\to G_{(k)}g_i.$$

于是ϕ是 $G^{(k)}$ 与集 $P=\{G_{(k)}g_1,G_{(k)}g_2,\cdots,G_{(k)}g_n\}$间的一个一一映射．事实上，因 $G_{(k)}g_i\cap G_{(k)}g_j=\phi(i\neq j)$，故$\phi$是 $G^{(k)}$到 P 的一个映射．$\forall G_{(k)}g_i\in P$，$\exists g_i^k\in G^{(k)}$，且 $g_i\in G_{(k)}g_i$，使得$\phi(g_i^k)=G_{(k)}g_i$，从而ϕ是满射．$\forall x^k,y^k\in G^{(k)}$，设$\phi(x^k)=\phi(y^k)=G_{(k)}g_i$，则 $x,y\in G_{(k)}g_i$，从而$x=x_1g_i$，$y=x_2g_i$，$x_1,x_2\in G_{(k)}$，因此$x_1^k=e$，$x_2^k=e$. 于是$x^k=(x_1g_i)^k\xlongequal{\text{由}G\text{是交换群}}x_1^kg_i^k=eg_i^k=g_i^k$，且 $y^k=(x_2g_i)^k=x_2^kg_i^k=eg_i^k=g_i^k$，所以 $x^k=y^k$. 即ϕ是单射．综上可见ϕ是$G^{(k)}$与P间的一个一一映射．于是$|G^{(k)}|=n=[G:G_{(k)}]$.

18. 解 不成立．例，设 $A=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\1&-1\end{pmatrix},\begin{pmatrix}1&0\\0&0\end{pmatrix}\right\}$，$H=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\1&-1\end{pmatrix}\right\}$.
$\forall x,y\in A$，规定A的元间的关系：$x\sim y\Leftrightarrow\exists h\in H$，使得 $x=hy$. 则

1) A对矩阵乘法不作成群.

2) H对矩阵乘法作成群.

3) $\sim$是A的元间的一个等价关系.

4) 由$\sim$决定的A的一个分类是：$\left[\begin{pmatrix}1&0\\0&1\end{pmatrix}\right]=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\1&-1\end{pmatrix}\right\}=H$，$\left[\begin{pmatrix}1&0\\0&0\end{pmatrix}\right]=\left\{\begin{pmatrix}1&0\\0&0\end{pmatrix}\right\}$. 这里，类$\left[\begin{pmatrix}1&0\\0&1\end{pmatrix}\right]$与类$\left[\begin{pmatrix}1&0\\0&0\end{pmatrix}\right]$所含元素的个数不相等.

事实上：

1） 因$\begin{pmatrix}1&0\\1&-1\end{pmatrix}\begin{pmatrix}1&0\\0&0\end{pmatrix}=\begin{pmatrix}1&0\\1&0\end{pmatrix}\overline{\in} A$，故 A 对矩阵乘法不作成群.

2） H 的乘法表是

	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\1&-1\end{pmatrix}$
$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\1&-1\end{pmatrix}$
$\begin{pmatrix}1&0\\1&-1\end{pmatrix}$	$\begin{pmatrix}1&0\\1&-1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$

又矩阵乘法满足结合律，H 有单位元$\begin{pmatrix}1&0\\0&1\end{pmatrix}$，且$\begin{pmatrix}1&0\\0&1\end{pmatrix}$，$\begin{pmatrix}1&0\\1&-1\end{pmatrix}$分别有逆元$\begin{pmatrix}1&0\\0&1\end{pmatrix}$，$\begin{pmatrix}1&0\\1&-1\end{pmatrix}$. 从而 H 是一个群.

3） ① $\forall x\in A$，$\exists\begin{pmatrix}1&0\\0&1\end{pmatrix}\in H$，使得 $x=\begin{pmatrix}1&0\\0&1\end{pmatrix}x$，从而 $x\sim x$. ② $\forall x,y\in A$，若 $x\sim y$，则 $\exists h\in H$，使得 $x=hy$. 因 H 是群．故 $\exists h^{-1}\in H$，使得 $y=h^{-1}x$，从而 $y\sim x$. ③ $\forall x,y,z\in A$，若 $x\sim y$，$y\sim z$，则 $\exists h_1,h_2\in H$，使得 $x=h_1y$，$y=h_2z$，于是 $x=h_1h_2z$. 因 H 是群，故 $h_1h_2\in H$，从而 $x\sim z$. 所以$\sim$是 A 的元间的一个等价关系.

4） $\left[\begin{pmatrix}1&0\\0&1\end{pmatrix}\right]=\left\{x\in A\,\middle|\,x\sim\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\}=\left\{x\in A\,\middle|\,\exists h\in H，使得\ x=h\begin{pmatrix}1&0\\0&1\end{pmatrix}=h\right\}=H$ $=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\1&-1\end{pmatrix}\right\}$. 又$\left[\begin{pmatrix}1&0\\0&0\end{pmatrix}\right]=\left\{x\in A\,\middle|\,x\sim\begin{pmatrix}1&0\\0&0\end{pmatrix}\right\}=\left\{x\in A\,\middle|\,\exists h\in H，使得\ x=h\begin{pmatrix}1&0\\0&0\end{pmatrix}=\begin{pmatrix}1&0\\0&0\end{pmatrix}\right\}=\left\{\begin{pmatrix}1&0\\0&0\end{pmatrix}\right\}$. 从而由等价关系$\sim$决定的 A 的一个分类是 $\left[\begin{pmatrix}1&0\\0&1\end{pmatrix}\right]$与$\left[\begin{pmatrix}1&0\\0&0\end{pmatrix}\right]$.

19. 证 （$\Leftarrow$） 若 G 的指数 $d=n$，则 $\forall a\in G$，$a^d=e$，即 $a^n=e$. 因 n 是使 $a^n=e$ 的最小正整数，故必有 G 的一个元 b，而 b 的阶为 n. 于是 $G=(b)$是循环群.

（$\Rightarrow$） 若 $G=(b)$是循环群．因$|G|=n$，故 $\forall a\in G$，由第七章，三，1，7），$a^n=e$. 假定 G 的指数 $d\neq n$，则 $d<n$，对 b 来说，有 $b^d=b^n=e$，即 $b^{n-d}=e$，$0<n-d<n$，此与$|b|=|G|=n$ 矛盾．所以 G 的指数 $d=n$.

20. 证 设 $a\in G$ 且$|a|=m$. $\forall x\in G$，因 G 是有限群，故 G 中任一元的阶都有限，可设$|x|=n$，往证 $n\,|\,m$. 事实上，由第七章，二，8，注 5）知，G 中存在阶为$[m,n]$的元．若$[m,n]\neq m$，则$[m,n]>m$，此与 m 是 G 中元的最大阶矛盾，从而$[m,n]=m$，于是 $n\,|\,m$.

注 该命题在非交换群中不成立．例，4 次对称群 S_4 中元(1 2 3 4)的阶为 4，4 是 S_4 中

元的最大阶．(1 2 3)($\in S_4$)的阶为 3，但 $3\nmid 4$.

21. 证 (反证法) 若$[H:K]<[N\cap H:N\cap K]$，则$\exists x_i,x_j\in N\cap H$，使得 $x_i(N\cap K)\neq x_j(N\cap K)$，但 $x_iK=x_jK$，从而 $x_i^{-1}x_j\overline{\in} N\cap K$，但 $x_i^{-1}x_j\in K$. 于是 $x_i^{-1}x_j\in K\cap N\cap H \xlongequal{\text{由}K<H} N\cap K$，此与 $x_i^{-1}x_j\overline{\in} N\cap K$ 矛盾．所以$[H:K]\geqslant[N\cap H:N\cap K]$.

22. 证一 设 H 的子群 $H\cap K$ 的所有不同左陪集为 $x_i(H\cap K)$，其中 $x_i\in H$ 且当 $x_i\neq x_j$ 时，$x_i^{-1}x_j\overline{\in} H\cap K$. 下面证明当 $x_i\neq x_j$ 时，$x_iK\neq x_jK$. 假设不然，由 $x_iK=x_jK$，得 $x_i^{-1}x_j\in K$，又 $x_i^{-1}x_j\in H$，于是 $x_i^{-1}x_j\in H\cap K$，产生矛盾．所以 x_iK 是G 的子群K 的不同的左陪集，从而证得 G 的子群 K 的左陪集数不小于 H 的子群 $H\cap K$ 的左陪集数，即$[G:K]\geqslant[H:H\cap K]$.

证二 令 A 是 H 的子群 $H\cap K$ 的所有右陪集组成的集合，B 是 G 的子群 K 的所有右陪集组成的集合．则$\phi:(H\cap K)h\to Kh(h\in H)$是 A 到 B 的单射．事实上，$\forall(H\cap K)h\in A$，$\exists Kh\in B$，使得$\phi((H\cap K)h)=Kh$. 若$(H\cap K)h'=(H\cap K)h$，则 $h'h^{-1}\in H\cap K\subset K$，从而 $Kh'=Kh$，所以ϕ是映射．$\forall(H\cap K)h,(H\cap K)h'\in A$，若 $Kh=Kh'$，则 $h'h^{-1}\in K$，又 $h'h^{-1}\in H$，于是 $h'h^{-1}\in H\cap K$，从而$(H\cap K)h=(H\cap K)h'$，所以ϕ是单射．因此 A 所含元的个数不大于 B 所含元的个数，即$[H:H\cap K]\leqslant[G:K]$.

第八章

1. 解 1) H 不是G 的不变子群．因为 $Hb=\{b,d\}\neq\{b,f\}=bH$.

2) $H\lhd G$. 事实上，$\forall\tau_{ab}\in G$，$\forall\tau_{1c}\in H$，$\forall x\in\mathbb{R}$. $x^{\tau_{ab}}=ax+b$，$x^{\tau_{1c}}=x+c$，$x^{\tau_{ab}^{-1}}=a^{-1}x-a^{-1}b$. $x^{\tau_{ab}\tau_{1c}\tau_{ab}^{-1}}=(x^{\tau_{ab}})^{\tau_{1c}\tau_{ab}^{-1}}=((ax+b)^{\tau_{1c}})^{\tau_{ab}^{-1}}=((ax+b)+c)^{\tau_{ab}^{-1}}=(ax+(b+c))^{\tau_{ab}^{-1}}=a^{-1}(ax+(b+c))-a^{-1}b=a^{-1}ax+a^{-1}b+a^{-1}c-a^{-1}b=x+a^{-1}c$. 因 $a^{-1}c\in\mathbb{Q}$，故 $\tau_{ab}\tau_{1c}\tau_{ab}^{-1}\in H$. 所以 $H\lhd G$.

2. 解 1) $|G/N|=\dfrac{|G|}{|N|}=\dfrac{9}{3}=3$，从而 G/N 含 3 个元．$G/N=\{[0]+N,[1]+N,[2]+N\}$，其中$[0]+N=N=([3])=\{[0],[3],[6]\}$，$[1]+N=\{[1],[4],[7]\}$，$[2]+N=\{[2],[5],[8]\}$.

2) $|G/N|=\dfrac{|G|}{|N|}=\dfrac{15}{5}=3$，从而 G/N 含 3 个元．$G/N=\{N,aN,a^2N\}$，其中 $N=(a^3)=\{a^3,a^6,a^9,a^{12},a^{15}=e\}$，$aN=a(a^3)=\{a^4,a^7,a^{10},a^{13},a^{16}=a\}$，$a^2N=a^2(a^3)=\{a^5,a^8,a^{11},a^{14},a^{17}=a^2\}$.

3) $G/N=\{a+N\mid a\in G,0\leqslant a<1\}$，其加法为：

$$(a+N)+(b+N)=\begin{cases}(a+b)+N, & a+b<1;\\(a+b-1)+N, & a+b\geqslant 1.\end{cases}$$

注 3)中的商群 G/N 是无限群，但它的每个元都是有限阶的．事实上，$\forall a+N\in G/N$，$a\in G$. 可设 $a=\frac{s}{t}$，则 $ta=s\in N$，于是 $t(a+N)=ta+N=N$，其中 N 是G/N 的单位元．所以 $a+N$ 的阶$\leqslant t$，是有限的.

3. 证 1) $|G/N|=\frac{|G|}{|N|}=\frac{24}{4}=6$. 从而 G/N 含 6 个元 . $G/N=\{(1)N,(1\ 2)N,(1\ 3)N,(2\ 3)N,(1\ 2\ 3)N,(1\ 3\ 2)N\}$，其中$(1)N=N$，$(1\ 2)N=\{(1\ 2),(3\ 4),(1\ 4\ 2\ 3),(1\ 3\ 2\ 4)\}$，$(1\ 3)N=\{(1\ 3),(1\ 4\ 3\ 2),(2\ 4),(1\ 2\ 3\ 4)\}$，$(2\ 3)N=\{(2\ 3),(1\ 2\ 4\ 3),(1\ 3\ 4\ 2),(1\ 4)\}$，$(123)N=\{(1\ 2\ 3),(2\ 4\ 3),(1\ 4\ 2),(1\ 3\ 4)\}$，$(132)N=\{(132),(143),(234),(124)\}$.
下面证明 $S_4/N\cong S_3$. $\forall aN\in S_4/N, a\in S_3$，则$\phi: aN\to a$ 是 S_4/N 与 S_3 间的一个同构映射 . 事实上，① $\forall aN\in S_4/N$，由于 $a\in S_3$，因此 $\exists\,|\,a\in S_3$，使得$\phi(aN)=a$. 从而ϕ是映射 . ② $\forall a\in S_3$，$\exists aN\in S_4/N$，使得$\phi(aN)=a$. 从而ϕ是满射 . ③ $\forall aN,bN\in S_4/N$，若 $a=b$，则 $aN=bN$. 从而ϕ是单射 . ④ $\forall aN,bN\in S_4/N$，$\phi(aN)=a$，$\phi(bN)=b$. 因$a,b\in S_3$，而 S_3 是群，故 $ab\in S_3$. 从而$\phi((aN)(bN))=\phi((ab)N)=ab=\phi(aN)\phi(bN)$. 所以 $S_4/N\overset{\phi}{\cong}S_3$.

2) $G/N=\left\{\begin{pmatrix}a & b\\0 & 1\end{pmatrix}N\,\middle|\,a,b\in\mathbf{Q},a\neq0\right\}$，其中 $\begin{pmatrix}a & b\\0 & 1\end{pmatrix}N=\left\{\begin{pmatrix}a & b\\0 & 1\end{pmatrix}\begin{pmatrix}1 & c\\0 & 1\end{pmatrix}\,\middle|\,c\in\mathbf{Q}\right\}=\left\{\begin{pmatrix}a & ac+b\\0 & 1\end{pmatrix}\,\middle|\,c\in\mathbf{Q}\right\}$. 因 $a\neq0$，c 跑遍所有的有理数，故 $ac+b$ 也跑遍所有的有理数，从而 $\begin{pmatrix}a & b\\0 & 1\end{pmatrix}N=\left\{\begin{pmatrix}a & d\\0 & 1\end{pmatrix}\,\middle|\,d\in\mathbf{Q}\right\}$. 由此说明，$\begin{pmatrix}a & b\\0 & 1\end{pmatrix}$所在的 N 的陪集由 a 唯一确定 . 所以 $G/N=\left\{\begin{pmatrix}a & 1\\0 & 1\end{pmatrix}N\,\middle|\,a\in\mathbf{Q},a\neq0\right\}$. 下面证明 $G/N\cong\overline{G}$. $\forall\begin{pmatrix}a & 1\\0 & 1\end{pmatrix}N\in G/N$，则 $\phi:\begin{pmatrix}a & 1\\0 & 1\end{pmatrix}N\to a$ 是G/N 与$\overline{G}$ 间的一个同构映射. 事实上，① $\forall\begin{pmatrix}a & 1\\0 & 1\end{pmatrix}N\in G/N$，使得 $a\in\overline{G}$，使得$\phi\left(\begin{pmatrix}a & 1\\0 & 1\end{pmatrix}\right)=a$. 若$\begin{pmatrix}a & 1\\0 & 1\end{pmatrix}N=\begin{pmatrix}a' & 1\\0 & 1\end{pmatrix}N$，则 $a=a'$. 从而ϕ是映射 . ② $\forall a\in\overline{G}$，$\exists\begin{pmatrix}a & 1\\0 & 1\end{pmatrix}N\in G/N$，使得$\phi\left(\begin{pmatrix}a & 1\\0 & 1\end{pmatrix}N\right)=a$. 从而$\phi$是满射 . ③ $\forall\begin{pmatrix}a & 1\\0 & 1\end{pmatrix}N,\begin{pmatrix}a' & 1\\0 & 1\end{pmatrix}N\in G/N$，若 $a=a'$，则$\begin{pmatrix}a & 1\\0 & 1\end{pmatrix}N=\begin{pmatrix}a' & 1\\0 & 1\end{pmatrix}N$. 从而$\phi$是单射 . ④ $\forall\begin{pmatrix}a & 1\\0 & 1\end{pmatrix}N,\begin{pmatrix}a' & 1\\0 & 1\end{pmatrix}N\in G/N$，有 $\phi\left(\left(\begin{pmatrix}a & 1\\0 & 1\end{pmatrix}N\right)\left(\begin{pmatrix}a' & 1\\0 & 1\end{pmatrix}N\right)\right)=\phi\left(\begin{pmatrix}aa' & a+1\\0 & 1\end{pmatrix}N\right)=\phi\left[\begin{pmatrix}aa' & 1\\0 & 1\end{pmatrix}\begin{pmatrix}1 & \frac{1}{a'}\\0 & 1\end{pmatrix}N\right]=\phi\left(\begin{pmatrix}aa' & 1\\ & 1\end{pmatrix}N\right)=aa'=\phi\left(\begin{pmatrix}a & 1\\0 & 1\end{pmatrix}N\right)\phi\left(\begin{pmatrix}a' & 1\\0 & 1\end{pmatrix}N\right)$.

4. 解 1) 不正确 . 例，取 $G=S_3$，$H_1=\{(1)\}$，$H_2=\{(1),(12)\}$，$H_3=S_3$. 虽 $H_1H_3=H_2H_3$，但 $H_1\neq H_2$.

2) 正确 . 证 . $\forall h_1h_3\in(H_1H_3)\cap H_2\cap H_4$，$h_1\in H_1$，$h_3\in H_3$，有 $h_1h_3\in H_1H_3$，$h_1h_3\in H_2$，$h_1h_3\in H_4$. 于是 $h_3\in h_1^{-1}H_2\subset H_2$，同样 $h_1\in H_4h_3^{-1}\subset H_4$，从而 $h_1\in H_1\cap H_4$，$h_3\in H_2\cap H_3$. 所以 $h_1h_3\in(H_1\cap H_4)(H_2\cap H_3)$. 另一方面，因 $H_1\cap H_4\subset H_1$，$H_2\cap H_3\subset H_3$，故 $(H_1\cap H_4)(H_2\cap H_3)\subset H_1H_3$. 又 $H_1\cap H_4\subset H_2\cap H_4$，$H_2\cap H_3\subset H_2\cap H_4$，从而$(H_1\cap H_4)\cdot(H_2\cap H_3)\subset(H_2\cap H_4)(H_2\cap H_4)\xlongequal{\text{由 } H_2\cap H_4<G}H_2\cap H_4$. 所以

$$(H_1 \cap H_4)(H_2 \cap H_3) \subset (H_1H_3) \cap H_2 \cap H_4.$$

因此等式得证.

3) 正确. 证一. 因 $H_1 \lhd G, H_3 \lhd G$,故由第八章,二,4,注10)知,$H_1H_3 \lhd G$. 因 $H_1 \subset H_2, H_3 \lhd G, H_2 < G$,故由第八章,二,4 知,$H_1H_3 \subset H_2H_3 < G$. 再由第八章,三,2,5)知,$H_1H_3 \lhd H_2H_3$.

证二 $e = ee \in H_1H_3 \neq \varnothing, H_1H_3 \subset H_2H_3$. $\forall h_1h_3, h_1'h_3' \in H_1H_3$,其中 $h_1, h_1' \in H_1, h_3, h_3' \in H_3$. $(h_1h_3)(h_1'h_3')^{-1} = h_1(h_3h_3'^{-1})h_1'^{-1}$. 因 $H_3 \lhd G$,故 $(h_3h_3'^{-1})h_1'^{-1} \in H_3h_1'^{-1} = h_1'^{-1}H_3$,从而 $\exists h_3'' \in H_3$,使得 $(h_3h_3'^{-1})h_1'^{-1} = h_1'^{-1}h_3''$. 于是 $(h_1h_3)(h_1'h_3')^{-1} = (h_1h_1'^{-1})h_3'' \in H_1H_3$. 所以 $H_1H_3 < H_2H_3$. 又 $\forall h_2h_3 \in H_2H_3, h_1h_3' \in H_1H_3$, $(h_2h_3)(h_1h_3')(h_2h_3)^{-1} = h_2(h_3h_1)h_3'h_3^{-1}h_2^{-1}$. 因 $H_1 \lhd G$,故 $h_3h_1 \in h_3H_1 = H_1h_3$,从而 $\exists h_1' \in H_1$,使得 $h_3h_1 = h_1'h_3$. 于是 $(h_2h_3)(h_1h_3')(h_2h_3)^{-1} = h_2h_1'(h_3h_3'h_3^{-1})h_2^{-1}$. 因 $H_3 \lhd G$,故 $(h_3h_3'h_3^{-1})h_2^{-1} \in H_3h_2^{-1} = h_2^{-1}H_3$,从而 $\exists h_3'' \in H_3$,使得 $(h_3h_3'h_3^{-1})h_2^{-1} = h_2^{-1}h_3''$. 于是 $(h_2h_3)(h_1h_3')(h_2h_3)^{-1} = (h_2h_1'h_2^{-1})h_3'' \in H_1H_3$(因 $H_1 \lhd G$). 所以 $H_1H_3 \lhd H_2H_3$.

5. 分析,HK 中含多少个元呢? 形式上看似乎是 $|H| \cdot |K|$. 但在 HK 中形如 $hk(h \in H, k \in K)$ 的元是否有重复的呢? 即当 $h' \neq h$ 或 $k' \neq k$ 时,是否有 $h'k' = hk$ 呢? 例,$H = \{(1),(1\ 2)\} < S_4, K = \{(1),(1\ 2),(3\ 4),(1\ 2)(3\ 4)\} < S_4$. 取 $h = (1), h' = (1\ 2) \in H, k = (3\ 4), k' = (1\ 2)(3\ 4) \in K$,有 $h' \neq h$,但 $h'k' = (1\ 2)(1\ 2)(3\ 4) = (3\ 4) = hk$. 因此可能发生重复情况. 即 $|HK|$ 未必等于 $|H| \cdot |K|$,而是 $|HK| \leqslant |H| \cdot |K|$. 我们知道 $|H| \cdot |K| = |H \times K|$,这里卡氏积 $H \times K = \left\{(h,k) \,\middle|\, h \in H, k \in K\right\}$,且 $(h,k) = (h',k') \Leftrightarrow h = h', k = k'$. 为了证明 $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$,只需证明,在 $H \times K$ 中,对于每 $(h_1,k_1) \in H \times K$,有且仅有 $|H \cap K| = s$ 个元 (h_i,k_i) $(i = 1,2,\cdots,s)$,使 $h_1k_1 = h_2k_2 = \cdots = h_sk_s (\in HK)$,即有且仅有 $|H \cap K| = s$ 个元重复.

证一 设 $H \cap K = \{d_1 = e, d_2, \cdots, d_s\}$. $\forall (h_1,k_1) \in H \times K$. 令 $h_i = h_1d_i^{-1}, k_i = d_ik_1$,显然 $h_i \in H, k_i \in K, i = 1,2,\cdots,s$,于是 $h_ik_i = h_1d_i^{-1}d_ik_1 = h_1k_1, i = 1,2,\cdots,s$. 且当 $i \neq j$ 时,$h_i \neq h_j$. 从而至少有 s 个元 $h_ik_i (\in HK, i = 1,2,\cdots,s)$ 重复. 另一方面,若 $(h',k') \in H \times K, h' \neq h_1$,而 $h'k' = h_1k_1$,则 $h_1^{-1}h' = k_1k'^{-1} \in H \cap K = \{d_1 = e, d_2, \cdots, d_s\}$,即 $h_1^{-1}h' = k_1k'^{-1} = d_i$,因此 $h' = h_1d_i, k' = d_i^{-1}k_1, i \in \{1,2,\cdots,s\}$. 从而至多有 s 个元 $hk (\in HK)$ 重复. 所以,在 $H \times K$ 中,对于每 $(h_1,k_1) \in H \times K$,有且仅有 $|H \cap K| = s$ 个元 $(h_i,k_i)(i = 1,2,\cdots,s)$,使 $h_1k_1 = h_2k_2 = \cdots = h_sk_s \in HK$. 于是 $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$.

证二 设卡氏积 $H \times K = \left\{(h,k) \,\middle|\, h \in H, k \in K\right\}$,且 $(h,k) = (h',k') \Leftrightarrow h = h', k = k'$. 已知 $|H \times K| = |H| \cdot |K|$. 对 $H \times K$ 引入一个关系:

$$(h,k) \sim (h',k') \Leftrightarrow hk = h'k'.$$

易证 $\sim$ 是 $H \times K$ 的元间的一个等价关系. 于是利用此等价关系 $\sim$ 可把 $H \times K$ 分成 $|HK|$ 个类. 取定 $(h_1,k_1) \in H \times K$,(h_1,k_1) 所在的等价类为:

$$[(h_1,k_1)] = \left\{(h,k) \in H \times K \,\middle|\, (h,k) \sim (h_1,k_1)\right\}.$$

下面考察类 $[(h_1,k_1)]$ 中含多少个元. $\forall (h,k) \in [(h_1,k_1)]$, $(h,k) \sim (h_1,k_1)$,即 $hk = h_1k_1$,从而 $h_1^{-1}h = k_1k^{-1} \in H \cap K$. 设 $H \cap K = \{d_1 = e, d_2, \cdots, d_s\}$,因此,$h_1^{-1}h = k_1k^{-1} = d_i, i \in$

$\{1,2,\cdots,s\}$，即 $h=h_1d_i, k=d_i^{-1}k_1$，也就是 $(h,k)=(h_1d_i,d_i^{-1}k_1)$. 所以 $[(h_1,k_1)]$ 中至多含 $|H\cap K|$ 个元．另一方面，$\forall d_i\in H\cap K$，有 $(h_1d_i,d_i^{-1}k_1)\in H\times K$. 因 $(h_1d_i)(d_i^{-1}k_1)=h_1k_1$，故 $(h_1d_i,d_i^{-1}k_1)\sim(h_1,k_1)$，从而 $(h_1d_i,d_i^{-1}k_1)\in[(h_1,k_1)]$，$i=1,2,\cdots,s$. 又 $\forall d_i,d_j\in H\cap K$，若 $d_i\neq d_j$，则 $(h_1d_i,d_i^{-1}k_1)\neq(h_1d_j,d_j^{-1}k_1)$. 所以 $[(h_1,k_1)]$ 中至少含 $|H\cap K|$ 个元. 综上可知，类 $[(h_1,k_1)]$ 中不同元的个数为 $|H\cap K|$. 于是 $|H|\cdot|K|=|H\times K|=|HK|\cdot|H\cap K|$，显然 $|H\cap K|\neq 0$，从而 $|HK|=\dfrac{|H|\cdot|K|}{|H\cap K|}$.

证三 因 $H<G,K<G$，故 $H\cap K<K$. 对 K 作关于 $H\cap K$ 的右陪集分解：$K=\bigcup\limits_{i=1}^{t}(H\cap K)k_i$，$k_i\in K$. 当 $i\neq j$ 时，$(H\cap K)k_i\cap(H\cap K)k_j=\varnothing$，$i,j=1,2,\cdots,t$. 作集 $A=\{hk_i|h\in H,i=1,2,\cdots,t\}$. 则 $HK=A$. 事实上，$\forall hk_i\in A$，有 $hk_i\in HK$，从而 $A\subset HK$. 反之，$\forall hk\in HK,h\in H,k\in K$，于是 $\exists i\in\{1,2,\cdots,t\}$，使得 $k\in(H\cap K)k_i$，因此 $\exists d\in H\cap K\subset H$，使得 $k=dk_i$，可见 $hk=(hd)k_i\in A$，从而 $HK\subset A$. 所以 $HK=A$. 又 A 中任意两个形如 hk_i 的元不相等．事实上，$\forall hk_i,h'k_j\in A,i\neq j,i,j=1,2,\cdots,t$. 若 $hk_i=h'k_j$，则 $k_ik_j^{-1}=h^{-1}h'\in H\cap K$，从而 k_i,k_j 在 $H\cap K$ 的同一个右陪集内，即 $(H\cap K)k_i=(H\cap K)k_j$，此与 $(H\cap K)k_i\cap(H\cap K)k_j=\varnothing$ 矛盾．所以 $hk_i\neq h'k_j$，$i\neq j$. 于是 A 中共有 $|H|t=|H|[K:H\cap K]$ 个不同的元，即 $|HK|=|H|[K:H\cap K]$. 由 Lagrange 定理，$|K|=|H\cap K|[K:H\cap K]$，显然 $|H\cap K|\neq 0$，从而 $[K:H\cap K]=\dfrac{|K|}{|H\cap K|}$，所以 $|HK|=\dfrac{|H|\cdot|K|}{|H\cap K|}$.

证四 因 $H<G,K<G$，故 $H\cap K<K$. 对 K 作关于 $H\cap K$ 的右陪集分解：$\exists k_i\in K$，$i=1,2,\cdots,t$，使得 $K=\bigcup\limits_{i=1}^{t}(H\cap K)k_i$. 当 $i\neq j$ 时，$(H\cap K)k_i\cap(H\cap K)k_j=\varnothing$，$i,j=1,2,\cdots,t$. 再由每个右陪集 $(H\cap K)k_i$ 都含 $|H\cap K|$ 个元，从而 $|K|=|H\cap K|t$，即 $t=\dfrac{|K|}{|H\cap K|}$. 用 H 左乘 $K=\bigcup\limits_{i=1}^{t}(H\cap K)k_i$ 的两端，得 $HK=\bigcup\limits_{i=1}^{t}H(H\cap K)k_i$. 因 $H\cap K\subset H,H<G$，故 $H(H\cap K)=H$，于是 $HK=\bigcup\limits_{i=1}^{t}Hk_i$. 且 $i\neq j$ 时，$Hk_i\cap Hk_j=\varnothing$，$i,j=1,2,\cdots,t$. 事实上，假设 $Hk_i\cap Hk_j\neq\varnothing$，则 $\exists h_1k_i=h_2k_j\in Hk_i\cap Hk_j$，其中 $h_1,h_2\in H,i\neq j$. 于是 $k_ik_j^{-1}=h_1^{-1}h_2\in H\cap K$，从而 k_i,k_j 在 $H\cap K$ 的同一个右陪集中，即 $(H\cap K)k_i=(H\cap K)k_j$，此与 $(H\cap K)k_i\cap(H\cap K)k_j=\varnothing$ 矛盾．所以 $Hk_i\cap Hk_j=\phi$，$i\neq j$. 又因每个右陪集 Hk_i 都含 $|H|$ 个元，故 $|HK|=|H|t=\dfrac{|H|\cdot|K|}{|H\cap K|}$.

注 1) 设 H 与 K 都是群 G 的有限子群，且 $H\cap K=\{e\}$，则 $|HK|=|H|\cdot|K|$.

2) 设 H 与 K 都是群 G 的有限子群，且 $(|H|,|K|)=1$，则 $|HK|=|H|\cdot|K|$.

证 因 $H<G,K<G$，故 $H\cap K<H$ 且 $H\cap K<K$. 从而 $|H\cap K|\,\big|\,|H|$ 且 $|H\cap K|\,\big|\,|K|$，于是 $|H\cap K|\,\big|\,(|H|,|K|)=1$，即 $H\cap K=\{e\}$，所以 $|HK|=|H|\cdot|K|$.

6. 证 设 G 有 2 个 3 阶子群 $H,K,H\neq K$，则 $H\cap K<H$，从而 $|H\cap K|\,\big|\,|H|=3$，于是 $|H\cap K|=1$ 或 3. 若 $|H\cap K|=3$，则 $H=H\cap K=K$，此与 $H\neq K$ 矛盾．因而 $|H\cap K|=1$，所以 $|HK|=|H|\cdot|K|=3\times3=9$. 但 $G\supset HK$，于是 $|G|\geqslant|HK|=9$，此与 $|G|=6$ 矛盾. 因而 G 至多含有一个 3 阶子群.

注 由第七章,四,15 知 6 阶群至少含有一个 3 阶子群,从而再结合本命题知,6 阶群有且只有一个 3 阶子群.

7. 证 对 n 作数学归纳法.

1) $n=2$ 时,由前面 5 题注 2)知,$|H_1H_2|=|H_1|\cdot|H_2|$.

2) 假定 $n-1$ 时,命题成立. 今看 n 时:已知 $H_i(i=1,2,\cdots,n)$ 是群 G 的有限子群,$|H_i|(i=1,2,\cdots,n)$ 两两互素. 由前面 5 题及归纳假定,且因 $H_i \lhd G(i=1,2,\cdots,n-1)$,故 $H_1H_2\cdots H_{n-1}$ 是 G 的有限子群,从而

$$|H_1H_2\cdots H_n|=|(H_1H_2\cdots H_{n-1})H_n|=\frac{|H_1H_2\cdots H_{n-1}|\cdot|H_n|}{|H_1H_2\cdots H_{n-1}\cap H_n|}$$

$$=\frac{|H_1|\cdot|H_2|\cdots|H_{n-1}|\cdot|H_n|}{|H_1H_2\cdots H_{n-1}\cap H_n|}.$$

因 $|H_i|$ 两两互素,故 $(|H_1|\cdot|H_2|\cdots|H_{n-1}|,|H_n|)=1$,由归纳假定,$|H_1|\cdot|H_2|\cdots|H_{n-1}|=|H_1H_2\cdots H_{n-1}|$,从而 $(|H_1H_2\cdots H_{n-1}|,|H_n|)=1$,由上面 5 题注 2),$|H_1H_2\cdots H_n|=|H_1|\cdot|H_2|\cdots|H_n|$.

8. 证 设 $H=(a)$. 因 S 是 H 的共轭子群,故 $\exists x\in G$,使得 $S=xHx^{-1}$(见第八章,一,7). 则 $S=(xax^{-1})$. 事实上,$\forall s\in S$,因 $S=xHx^{-1}$,故 $\exists h\in H$,使得 $s=xhx^{-1}$. 因 $H=(a)$,故 $\exists n\in\mathbb{Z}$,使得 $h=a^n$,从而 $s=xa^nx^{-1}=(xax^{-1})^n\in(xax^{-1})$,于是 $S\subset(xax^{-1})$. 反之,因 $xax^{-1}\in xHx^{-1}=S$,又 $S<G$,故 $(xax^{-1})\subset S$. 所以 $S=(xax^{-1})$.

9. 解 首先作出包含子集 S 的群 G 的子集:$S_0=\{gsg^{-1}|s\in S,g\in G\}\neq\varnothing$. 则由 S_0 生成的子群 (S_0) 就是包含 S 的 G 的最小不变子群. 事实上,显然 $(S_0)<G$. 又 $\forall s\in S$,$s=ese^{-1}\in S_0\subset(S_0)$,从而 $(S_0)\supset S$. $\forall a\in G$,$\forall x_1x_2\cdots x_n\in(S_0)$,$x_i\in S_0\cup S_0^{-1}$,其中 $S_0^{-1}=\{s^{-1}|s\in S_0\}$(见第七章,一,3). 有 $a(x_1x_2\cdots x_n)a^{-1}=(ax_1a^{-1})(ax_2a^{-1})\cdots(ax_na^{-1})$. 当 $x_i\in S_0$ 时,$x_i=gsg^{-1}$,其中 $g\in G,s\in S$,从而 $ax_ia^{-1}=agsg^{-1}a^{-1}=(ag)s(ag)^{-1}$,其中 $ag\in G,s\in S$,因此 $ax_ia^{-1}\in S_0$. 当 $x_i\in S_0^{-1}$ 时,$x_i^{-1}\in S_0$,于是 $x_i^{-1}=g's'g'^{-1}$,其中 $g'\in G,s'\in S$,从而 $ax_i^{-1}a^{-1}=ag's'g'^{-1}a^{-1}=(ag')s'(ag')^{-1}$,其中 $ag'\in G,s'\in S$,因此 $ax_i^{-1}a^{-1}\in S_0$,可见 $ax_ia^{-1}=(ax_i^{-1}a^{-1})^{-1}\in(S_0)$. 所以 $a(x_1x_2\cdots x_n)a^{-1}\in(S_0)$. 从而证得 $(S_0)\lhd G$. $\forall N\lhd G$,$N\supset S$,显然 $N\supset S_0$,于是 $N\supset(S_0)$. 所以 (S_0) 是包含 S 的 G 的最小不变子群.

将 (S_0) 称为由 S 生成的不变子群.

10. 证 设 $\pi=\begin{pmatrix}i_1 & i_2 & \cdots & i_n\\ i_1^\pi & i_2^\pi & \cdots & i_n^\pi\end{pmatrix}$. 已知 $(i_1\quad i_2\quad\cdots\quad i_k)=\begin{pmatrix}i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_n\\ i_2 & i_3 & \cdots & i_1 & i_{k+1} & \cdots & i_n\end{pmatrix}$.

令 $\sigma=(i_1\quad i_2\quad\cdots\quad i_k)$. 显然有 $(i_j^\pi)^{\pi^{-1}\sigma\pi}=i_j^{\sigma\pi}$,即 i_j^π 经置换 $\pi^{-1}\sigma\pi$ 作用后的象为 $i_j^{\sigma\pi}$,$j=1,2,\cdots,n$. 从而

$$\pi^{-1}\sigma\pi=\begin{pmatrix}i_1^\pi & i_2^\pi & \cdots & i_k^\pi & i_{k+1}^\pi & \cdots & i_n^\pi\\ i_1^{\sigma\pi} & i_2^{\sigma\pi} & \cdots & i_k^{\sigma\pi} & i_{k+1}^{\sigma\pi} & \cdots & i_n^{\sigma\pi}\end{pmatrix}$$

$$=\begin{pmatrix}i_1^\pi & i_2^\pi & \cdots & i_k^\pi & i_{k+1}^\pi & \cdots & i_n^\pi\\ i_2^\pi & i_3^\pi & \cdots & i_1^\pi & i_{k+1}^\pi & \cdots & i_n^\pi\end{pmatrix}=(i_1^\pi\quad i_2^\pi\quad\cdots\quad i_k^\pi).$$

11. 证 $\forall\pi=\begin{pmatrix}1 & 2 & \cdots & n\\ 1^\pi & 2^\pi & \cdots & n^\pi\end{pmatrix}\in Z$,$\forall\sigma\in S_n$,都有 $\sigma\pi=\pi\sigma$,即 $\pi^{-1}\sigma\pi=\sigma$. 因 $n\geqslant3$,故可取 $\sigma=(ij)$,于是 $\pi^{-1}(ij)\pi=(ij)$. 又由上面 10 题知,$\pi^{-1}(ij)\pi=(i^\pi j^\pi)$. 从而 $(i^\pi j^\pi)=$

$(ij), i,j=1,2,\cdots,n$. 因此, $(1^\pi 2^\pi)=(1\ 2)$, $(1^\pi 3^\pi)=(1\ 3)$, $\cdots$, $(1^\pi n^\pi)=(1\ n)$. 由此可知 $1^\pi=1, 2^\pi=2, \cdots, n^\pi=n$. 事实上,假设 $1^\pi\neq 1, 2^\pi\neq 1$,则 $1^{(1^\pi 2^\pi)}=1$,又 $1^{(12)}=2$. 因 $(1^\pi 2^\pi)=(1\ 2)$,故 $1=2$,矛盾. 所以 $1^\pi=1$ 或 $2^\pi=1$. 若 $2^\pi=1$,当然 $1^\pi\neq 1$. 因 $n\geqslant 3$,故 $\exists (1^\pi 3^\pi)=(1\ 3)$ 且 $3^\pi\neq 1$,从而 $1^{(1^\pi 3^\pi)}=1$,又 $1^{(1\ 3)}=3$,于是 $1=3$,矛盾. 所以 $2^\pi\neq 1$,只能 $1^\pi=1$. 类似地可证 $2^\pi=2, \cdots, n^\pi=n$. 从而 $\pi=(1)$. 所以 $Z=\{(1)\}$.

12. 证一 (反证法)假设 $G/Z=(aZ)$ 是循环群. $\forall x,y\in G$,有 $xz, yz\in G/Z$,即 $xZ=(aZ)^k=a^kZ$, $yZ=(aZ)^h=a^hZ$,从而 $x\in a^kZ$, $y\in a^hZ$,于是 $\exists z_1,z_2\in Z$,使得 $x=a^kz_1$, $y=a^hz_2$. 因此, $xy=a^kz_1a^hz_2=a^ka^hz_1z_2=a^ha^kz_2z_1=a^hz_2a^kz_1=yx$. 可见 G 是交换群,此与已知矛盾. 所以 G/Z 不是循环群.

证二 (反证法)设 $G/Z=(aZ)$ 是循环群,则 $G=(Z\cup\{a\})$. 事实上, $\forall g\in G$,有 $g=ge\in gZ$,又 $gZ\in G/Z$,从而 $\exists$ 整数 m,使得 $gZ=(aZ)^m=a^mZ$. 又 $a^mZ\subset(Z\cup\{a\})$,所以, $g\in(Z\cup\{a\})$,于是 $G\subset(Z\cup\{a\})$. 反之,显然 $(Z\cup\{a\})\subset G$. 因此 $G=(Z\cup\{a\})$. 由 Z 是交换群,又 $\forall z\in Z$,有 $za=az$,从而 $(Z\cup\{a\})$ 是交换群,即 G 是交换群,此与已知矛盾. 所以 G/Z 不是循环群.

注 该命题可作如下推广:设 $H<G$, Z 是 G 的中心, $H\subset Z$,则 $H\lhd G$. 此时,若 G 为非交换群,则 G/H 不是循环群.

证 $\forall g\in G, h\in H\subset Z$,有 $ghg^{-1}=hgg^{-1}=h\in H$,因此 $H\lhd G$. 从而 G/H 是商群. 假设 G/H 是循环群,则 $\exists a\in G$,使得 $G/H=(aH)$. $\forall g_1. g_2\in G$,有 $g_1H, g_2H\in G/H$,即 $g_1H=(aH)^{t_1}=a^{t_1}H$, $g_2H=(aH)^{t_2}=a^{t_2}H$,从而 $g_1\in a^{t_1}H$, $g_2\in a^{t_2}H$,于是 $\exists h_1,h_2\in H$,使得 $g_1=a^{t_1}h_1$, $g_2=a^{t_2}h_2$. 因此,由 H 中的元与 G 中的元可交换,且 a^{t_1} 与 a^{t_2} 可交换,有 $g_1g_2=a^{t_1}h_1a^{t_2}h_2=a^{t_1}a^{t_2}h_1h_2=a^{t_2}a^{t_1}h_2h_1=a^{t_2}h_2a^{t_1}h_1=g_2g_1$. 从而 G 是交换群. 此与已知矛盾. 所以 G/H 不是循环群.

13. 证 $\forall \begin{pmatrix}a & b\\ c & d\end{pmatrix}\in Z$,取 $\begin{pmatrix}x_1 & 0\\ 0 & x_2\end{pmatrix}\in GL_2(\mathbf{R})$,其中 $x_1\neq x_2$,有 $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}x_1 & 0\\ 0 & x_2\end{pmatrix}=\begin{pmatrix}x_1 & 0\\ 0 & x_2\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}$,即 $\begin{pmatrix}ax_1 & bx_2\\ cx_1 & dx_2\end{pmatrix}=\begin{pmatrix}x_1a & x_1b\\ x_2c & x_2d\end{pmatrix}$,从而 $bx_2=x_1b$, $cx_1=x_2c$. 因 $x_1\neq x_2$,故 $b=c=0$. 于是 $\begin{pmatrix}a & b\\ c & d\end{pmatrix}=\begin{pmatrix}a & 0\\ 0 & d\end{pmatrix}$ 是对角矩阵. 再取 $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\in GL_2(\mathbf{R})$,有 $\begin{pmatrix}a & 0\\ 0 & d\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}a & 0\\ 0 & d\end{pmatrix}$,即 $\begin{pmatrix}0 & a\\ d & 0\end{pmatrix}=\begin{pmatrix}0 & d\\ a & 0\end{pmatrix}$,从而 $d=a$. 于是 $\begin{pmatrix}a & b\\ c & d\end{pmatrix}=\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}$ 是纯量矩阵,所以 $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\left\{\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}\middle| a\in\mathbf{R}, a\neq 0\right\}$. 反之,任一 $\mathbf{R}$ 上的2阶可逆纯量矩阵 A 与任 $B\ (\in GL_2(\mathbf{R}))$ 都可交换,所以 $A\in Z$. 因此 $Z=\left\{\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}\middle| a\in\mathbf{R}, a\neq 0\right\}$.

注 此命题可推广为:当 $n\geqslant 2$ 时, $GL_n(\mathbf{R})$ 的中心由所有 $\mathbf{R}$ 上的 n 阶可逆纯量矩阵组成.

14. 解 $\forall (x,y)\in Z((1,1))$,有 $(1,1)(x,y)=(x,y)(1,1)$. 从而 $(x,x+y)=(x,y+1)$,即 $x+y=y+1$,于是 $x=1$. 所以 $Z((1,1))=\{(1,y)\mid y\in\mathbf{R}\}$.

15. 证 设$|a|=k$,则$\exists q,r\in\mathbb{Z}$,使得$k=qn+r,0\leqslant r<n$. 于是$a^k=(a^n)^q a^r$,即$a^r=(a^n)^{-q}a^k$. 因$a^n\in H,a^k=e\in H$,故$a^r\in H$,从而$r=0$. 因此$n\,|\,k$. 在G/H中,$aH,(aH)^2=a^2H,\cdots,(aH)^{n-1}=a^{n-1}H$都不等于$G/H$的单位元$H$,而$(aH)^n=a^nH=H$,因此$|aH|=n$.

16. 证 因$e\in H=\{x\in G\mid |x|有限\}$,故$H\neq\varnothing$. 显然$H\subset G$. $\forall a,b\in H$,设$|a|=n$,$|b|=m$,则$(ab)^{mn}\xlongequal{由G是交换群}a^{mn}b^{mn}=(a^n)^m(b^m)^n=e$,从而$|ab|$有限,因此$ab\in H$. 由第七章,二,5,$H<G$. 因$G$是交换群,故$H\lhd G$. $\forall aH\in G/H$,若$|aH|$有限,令$|aH|=s$,则$a^sH=(aH)^s=H$,从而$a^s\in H$,即$|a^s|$有限. 于是$\exists$正整数t,使得$(a^s)^t=a^{st}=e$,即$|a|$有限,因此$a\in H$,即$aH=H$是G/H的单位元. 所以G/H中除单位元外,所有元的阶都是无限的.

17. 证 ($\Rightarrow$) 因$N\lhd G$,故$\forall a\in G,aN=Na$,取$b=a$,有$aN=Nb$. ($\Leftarrow$) $\forall a\in G$,$\exists b\in G$,使得$aN=Nb$,从而$a\in Nb$,于是$Na=Nb$. 又$Nb=aN$,因此$Na=aN,\forall a\in G$. 所以$N\lhd G$.

18. 证 $\forall x\in N_1,y\in N_2$,要证$xy=yx$,只需证$x^{-1}y^{-1}xy=e$. 因$N_1\lhd G$,故$x^{-1}(y^{-1}xy)\in N_1$,因$N_2\lhd G$,故$(x^{-1}y^{-1}x)y\in N_2$,从而$x^{-1}y^{-1}xy\in N_1\cap N_2=\{e\}$. 于是$x^{-1}y^{-1}xy=e$,所以$xy=yx$.

注 1) 在该命题中,把条件$N_1\cap N_2=\{e\}$去掉,即使N_1与N_2都是交换群,结论也未必成立. 例,$G=\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\pm\begin{pmatrix}i&0\\0&-i\end{pmatrix},\pm\begin{pmatrix}0&1\\-1&0\end{pmatrix},\pm\begin{pmatrix}0&i\\i&0\end{pmatrix}\right\}$对于矩阵乘法作成一个群. $N_1=\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\pm\begin{pmatrix}i&0\\0&-i\end{pmatrix}\right\},N_2=\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\pm\begin{pmatrix}0&1\\-1&0\end{pmatrix}\right\}$. $N_1<G,N_2<G$. 因$[G:N_1]=[G:N_2]=\frac{8}{4}=2$,故由第八章,二,3,$N_1\lhd G,N_2\lhd G$(见第八章,三,10). $N_1\cap N_2=\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\}\neq\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\}$. 4阶群$N_1$与$N_2$都是交换群. $\begin{pmatrix}i&0\\0&-i\end{pmatrix}\in N_1,\begin{pmatrix}0&1\\-1&0\end{pmatrix}\in N_2$,但$\begin{pmatrix}i&0\\0&-i\end{pmatrix}\begin{pmatrix}0&1\\-1&0\end{pmatrix}=\begin{pmatrix}0&i\\i&0\end{pmatrix}\neq\begin{pmatrix}0&-i\\-i&0\end{pmatrix}=\begin{pmatrix}0&1\\-1&0\end{pmatrix}\begin{pmatrix}i&0\\0&-i\end{pmatrix}$.

2) 设$N_1\lhd G,N_2\lhd G$且$N_1\cap N_2=\{e\}$. 虽$\forall x\in N_1,y\in N_2$,都有$xy=yx$. 但$N_1N_2$未必是交换群. 例,$\{(1)\}\lhd S_3,S_3\lhd S_3,\{(1)\}\cap S_3=\{(1)\}$. 而$\{(1)\}S_3=S_3$不是交换群.

3) 设$N_1\lhd G,N_2\lhd G$且$N_1\cap N_2=\{e\}$. 若N_1与N_2都是交换群,显然N_1N_2也是交换群.

4) 设Z是G的中心,H是G的交换子群,则ZH是G的交换子群.

证 因$Z\lhd G,H<G$,故由第八章,二,4,$ZH<G$. $\forall z_1h_1,z_2h_2\in ZH,(z_1h_1)(z_2h_2)=z_1(h_1z_2)h_2=z_1(z_2h_1)h_2=(z_1z_2)(h_1h_2)=(z_2z_1)(h_2h_1)=z_2(z_1h_2)h_1=z_2(h_2z_1)h_1=(z_2h_2)(z_1h_1)$. 所以$ZH$是$G$的交换子群.

5) 设$N_1\lhd G,N_2\lhd G$,且$\forall a\in G$,都有唯一的$n_1\in N_1,n_2\in N_2$,使得$a=n_1n_2$. 则$\forall x\in N_1,y\in N_2$,都有$xy=yx$.

证 我们来证明$N_1\cap N_2=\{e\}$. $\forall b\in N_1\cap N_2$,显然$b\in G$,有$b=eb=be$. 由已知:G中元b表成N_1与N_2中元的积的唯一性,有$b=e$. 所以$N_1\cap N_2=\{e\}$. 从而结论成立.

19. 证 因$C\cap A<G,C\cap B<G$,又$A\lhd B$,故$C\cap A<C\cap B$. $\forall x\in C\cap B,\forall y\in C\cap A$.

因$x\in C$,$y\in C$,又$C<G$,故$xyx^{-1}\in C$;因$x\in B$,$y\in A$,又$A\lhd B$,故$xyx^{-1}\in A$.从而$xyx^{-1}\in C\cap A$.所以,$C\cap A\lhd C\cap B$.

20. 证一 因$H\lhd G$,$K\lhd G$,故$H\cap K\lhd G$.$\forall a,b\in G$,因G/H,G/K是交换群,故$Hab=(Ha)(Hb)=(Hb)(Ha)=Hba$,$Kab=(Ka)(Kb)=(Kb)(Ka)=Kba$.从而由第七章,四,14,$[(H\cap K)a]\cdot[(H\cap K)b]=(H\cap K)ab=Hab\cap Kab=Hba\cap Kba=(H\cap K)ba=[(H\cap K)b][(H\cap K)a]$.所以$G/H\cap K$是交换群.

证二 因$H\lhd G$,$K\lhd G$,故$H\cap K\lhd G$,从而$G/H\cap K$是商群.设C是由G中元的所有换位子生成的子群(见第八章,二,6,注2)).因G/H,G/K是交换群,故由第八章二,6,得$H\supset C$,$K\supset C$.于是$H\cap K\subset C$.从而$\forall a,b\in G$,由$a^{-1}b^{-1}ab\in H\cap K$,有$a^{-1}b^{-1}ab(H\cap K)=H\cap K$,即$ab(H\cap K)=ba(H\cap K)$.因此,$[a(H\cap K)][b(H\cap K)]=ab(H\cap k)=ba(H\cap K)=[b(H\cap K)][a(H\cap K)]$.所以$G/H\cap K$是交换群.

21. 证 ($\Leftarrow$) 由Lagrange定理,G的子群的阶是$|G|$的因子,而$|G|=$素数p的因子只有1与p,因此G的子群有且只有$\{e\}$与G.所以结论成立.

($\Rightarrow$) 因G是单群,故$|G|\neq 1$.假设$|G|$不是素数,又G是有限群,则$|G|$是合数.于是$\exists a\in G$,$a\neq e$.若$|a|<|G|$,则$(a)<G$,且$(a)\neq G$,$(a)\neq\{e\}$.又因G是交换群,故$(a)\lhd G$.此与已知矛盾.若$|a|=|G|=n$,取n的一个真因子k,$1<k<n$.从而$|a^k|=\dfrac{|a|}{(|a|,k)}=\dfrac{n}{k}$.

因$1<\dfrac{n}{k}<n$,故$(a^k)\neq\{e\}$且$(a^k)\neq G$.又$(a^k)\lhd G$.此与已知矛盾.

22. 证一 因$G\sim\overline{G}$,故存在G到$\overline{G}$的一个同态满射ϕ.设$\overline{N}$是$\overline{G}$的任一不变子群,则$\phi^{-1}(\overline{N})=N$是$G$的不变子群[①].因$G$是单群,故$N=\{e\}$或$N=G$.从而$\overline{N}=\{\bar{e}\}$或$\overline{N}=\overline{G}$.所以$\overline{G}$是单群或$\overline{G}=\{\bar{e}\}$.

证二 因$G\sim\overline{G}$,故存在G到$\overline{G}$的一个同态满射ϕ.设$N=\ker\phi$,则$N\lhd G$.由G是单群,从而N是$\{e\}$或是G.若$N=\{e\}$,则$G/N=G/\{e\}\cong G$.由同态基本定理,$G/N\cong G$[②],于是$G\cong\overline{G}$.因G是单群,故$\overline{G}$也是单群.若$N=G$,则$G/N=G/G=\{G\}$.由同态基本定理,$G/N\cong\overline{G}$,即$\overline{G}\cong\{G\}$.所以$\overline{G}=\{\bar{e}\}$,其中$\bar{e}$是$\overline{G}$的单位元.

注 设群$G\sim$群$\overline{G}$.若$\overline{G}$是单群,但G未必是单群.例,$\phi:a\to[a]$是$\mathbb{Z}$到$\mathbb{Z}_2$的同态满射,$\mathbb{Z}_2$是单射,但$\mathbb{Z}$不是单群.

23. 证一 因$N\lhd G$,$H<G$,故由第八章,二,4,$HN<G$.由Lagrange定理,$|HN|\,\big|\,|G|$.由第八章,四,5,$|HN|=\dfrac{|H||N|}{|H\cap N|}$,从而$\dfrac{|H||N|}{|H\cap N|}\,\Big|\,[G:N]|N|$.于是$\exists k\in\mathbb{Z}$,使得$[G:N]\cdot|N|\cdot|H\cap N|=|H|\cdot|N|\cdot k$.因$|N|\neq 0$,故$[G:N]\cdot|H\cap N|=|H|k$,从而$|H|\,\big|\,[G:N]\cdot|H\cap N|$.已知$(|N|,[G:N])=1$,又$|H|\,\big|\,|N|$,有$(|H|,[G:N])=1$(不然,若$(|H|,[G:N])=t\neq 1$,则$t\,\big|\,|H|$,又$|H|\,\big|\,|N|$,从而$t\,\big|\,|N|$且$t\,\big|\,[G:N]$,此与$(|N|,[G:N])=1$矛盾).所以$|H|\,\big|\,|H\cap N|$.但$H\cap N<H$,于是$|H\cap N|\,\big|\,|H|$.因此$|H|=|H\cap N|$.所以$H=H\cap N$.从而

① 张禾瑞.近世代数基础.北京:高等教育出版社,1978.78.定理4.

② 同上.76.定理2.

$H\subset N$. 即得 $H<N$.

证二 因 G 是有限群，$H<G$，故可设 $|H|=s$，$H=\{h_1=e,h_2,\cdots,h_s\}$，其中 $h_i\neq h_j(i\neq j,i,j=1,2,\cdots,s)$. 作集 $A=\{Nh_1,Nh_2,\cdots,Nh_s\}$. 显然 $\varnothing\neq A\subset G/N$. $\forall Nh_i,Nh_j\in A,h_i,h_j\in H$，因 $H<G$，故 $h_ih_j\in H$. 又由 $N\lhd G$，有 $(Nh_i)(Hh_j)=N(h_ih_j)\in A$. 因 A 是有限集，故 $A<G/N$. 所以 $|A|\mid|G/N|=[G:N]$. 因 $N\lhd G,H<G$，故由第八章，二，4，$NH<G$，即 $N\subset NH<G,N\lhd G$，由第八章，三，2，5)，$N\lhd NH$. 所以 NH/N 是商群. 由第八章，四，5，$|NH/N|=\frac{|NH|}{|N|}=\frac{|N||H|}{|N||N\cap H|}=\frac{|H|}{|N\cap H|}=\frac{s}{|N\cap H|}$. 又显然 $A<NH/N$，所以 $|A|\,\Big|\,\frac{s}{|N\cap H|}$. 已知 $([G:N],|N|)=1$，$s\,\Big|\,|N|$，有 $([G:N],s)=1$. 又 $\frac{s}{|N\cap H|}\,\Big|\,s$，所以 $\left([G:N],\frac{s}{|N\cap H|}\right)=1$. 于是 $|A|\,\Big|\left([G:N],\frac{s}{|N\cap H|}\right)=1$，从而 $|A|=1$. 即 $Nh_1=Nh_2=\cdots=Nh_s$，因此，$h_1,h_2,\cdots,h_s\in N$，从而 $H\subset N$，得 $H<N$.

24. 证 已知 H 是有限群，$K\lhd H$. 因 $H\lhd G$，故 $\forall g\in G,gKg^{-1}<gHg^{-1}=H$. 因 $[H:K]=|H/K|=\frac{|H|}{|K|}=\frac{nm}{n}=m$，故 $(|K|,[H:K])=(n,m)=1$. 由第八章，一，7，$|gKg^{-1}|=|K|$，当然 $|gKg^{-1}|\,\Big|\,|K|$. 因此由上面 23 题知，$gKg^{-1}<K$. 又 $|gKg^{-1}|=|K|$，所以 $gKg^{-1}=K$. 由 g 的任意性知 $K\lhd G$.

25. 证 (反证法)假设 $[G:H]$ 有限，设 $[G:H]=n$. 又已知 $H\lhd G$，从而 G/H 是商群，且 $|G/H|=n$. $\forall a\in G,Ha\in G/H$，由第七章，三，1，7)，$(Ha)^n=H$，又 $(Ha)^n=Ha^n$，即 $Ha^n=H$，从而 $a^n\in H$. $\forall g\in G$，由已知，$\exists b\in G$，使得 $b^n=g$. 因 $b^n\in H$，故 $g\in H$，所以 $G\subset H$. 又显然 $H\subset G$，从而 $H=G$. 此与已知 $H\neq G$ 矛盾. 于是 $[G:H]=\infty$.

26. 证 1) 因 F 是交换群，$H<F$，故 $H\lhd F$. $\forall g\in F$，$\forall$ 自然数 n，$\exists\,\frac{g}{n}\in F$，使得 $n\left(\frac{g}{n}\right)=g$. 从而方程 $nx=g$ 在 F 内恒有解. 由上面 25 题知，$\forall H<F,H\neq F$，有 $[F:H]=\infty$.

2) 因 M 是交换群，$H<M$，故 $H\lhd M$. $\forall A\in M$，$\forall$ 自然数 n，$\exists\,\frac{1}{n}A\in M$，使得 $n\left(\frac{1}{n}A\right)=A$. 从而方程 $nx=A$ 在 M 内恒有解. 由上面 25 题知，$\forall H<M,H\neq M$，有 $[M:H]=\infty$.

3) 因 $F[x]$ 是交换群，$H<F[x]$，故 $H\lhd F[x]$. $\forall f(x)\in F[x]$，$\forall$ 自然数 n，$\exists\,\frac{1}{n}f(x)\in F[x]$，使得 $n\left(\frac{1}{n}f(x)\right)=f(x)$. 从而方程 $ny=f(x)$ 在 $F[x]$ 内恒有解. 由上面 25 题知，$\forall H<F[x],H\neq F[x]$，有 $[F[x]:H]=\infty$.

注 1) 数域 F 的每个子加群($\neq F$)的指数都无限. 数域 F 上全体 n 阶矩阵集 M 的每个子加群($\neq M$)的指数都无限. 数域 F 上全体一元多项式集 $F[x]$ 的每个子加群($\neq F[x]$)的指数都无限.

2) 该命题中的数域 F 可以推广为特征为无限大的任意的一个域.

27. 证 1) $[a,b]^{-1}=(a^{-1}b^{-1}ab)^{-1}=b^{-1}a^{-1}ba=[b,a]$.

2)
$$[ab,c] = (ab)^{-1}c^{-1}ab\,c = b^{-1}a^{-1}c^{-1}a\,b\,c.$$
$$b^{-1}[a,c]b[b,c] = b^{-1}a^{-1}c^{-1}acbb^{-1}c^{-1}bc = b^{-1}a^{-1}c^{-1}abc.$$
$$[a,c]\big[[a,c],b\big][b,c] = [a,c][a,c]^{-1}b^{-1}a^{-1}c^{-1}acbb^{-1}c^{-1}bc = b^{-1}a^{-1}c^{-1}abc.$$

所以
$$[ab,c] = b^{-1}[a,c]b[b,c] = [a,c]\big[[a,c],b\big][b,c].$$

3) $[a,bc]\overset{由1)}{=\!=}[bc,a]^{-1}\overset{由2)}{=\!=}(c^{-1}[b,a]c[c,a])^{-1}=[c,a]^{-1}c^{-1}[b,a]^{-1}c$
$=[a,c]c^{-1}[a,b]c.$

$[a,c][a,b]\big[[a,b],c\big]=[a,c][a,b][a,b]^{-1}c^{-1}[a,b]c=a^{-1}c^{-1}acc^{-1}a^{-1}b^{-1}a\,b\,c$
$=a^{-1}(bc)^{-1}abc=[a,bc].$

所以
$$[a,bc] = [a,c]c^{-1}[a,b]c = [a,c][a,b]\big[[a,b],c\big].$$

4) $ab[a,b](ab)^{-1}=aba^{-1}b^{-1}abb^{-1}a^{-1}=aba^{-1}b^{-1}=[a^{-1},b^{-1}].$

5) $b[b,a]b^{-1}=bb^{-1}a^{-1}bab^{-1}=a^{-1}bab^{-1}=[a,b^{-1}].$

6) $[a^{-1},b]\overset{由1)}{=\!=}[b,a^{-1}]^{-1}\overset{由5)}{=\!=}(a[a,b]a^{-1})^{-1}\overset{由1)}{=\!=}a[b,a]a^{-1}.$

7) $[ab,c]\overset{由2)}{=\!=}b^{-1}[a,c]b[b,c]=b^{-1}b[a,c][b,c]=[a,c][b,c].$

8) $[a,bc]\overset{由1)}{=\!=}[bc,a]^{-1}\overset{由7)}{=\!=}([b,a][c,a])^{-1}\overset{由1)}{=\!=}[a,c][a,b]=[a,b][a,c].$

9) $[a^{-1},b^{-1}]\overset{由4)}{=\!=}ab[a,b](ab)^{-1}=ab(ab)^{-1}[a,b]=[a,b].$

10) $\big[[a,b],c\big]=[a,b]^{-1}c^{-1}[a,b]c=[a,b]^{-1}[a,b]c^{-1}c=e.$ $\big[a,[b,c]\big]=$
$a^{-1}[b,c]^{-1}a[b,c]=a^{-1}a[b,c]^{-1}[b,c]=e.$ 所以$\big[[a,b],c\big]=\big[a,[b,c]\big].$

11) $[a,b]^{-1}c\overset{由1)}{=\!=}[b,a]c=c[b,a]\overset{由1)}{=\!=}c[a,b]^{-1}.$

28. 证 因 $N\lhd G$, N 在 G 里的指数是 n, 故 G/N 是商群, 且 $|G/N|=n$. 又因 h 是使 $t^h\in N$ 的最小正整数, 故 $Nt\in G/N$, 且 $|Nt|=h$. 事实上, $(Nt)^h=Nt^h=N$. $\forall$ 正整数 k, $k<h$, 因 $t^k\overline{\in} N$, 故 $(Nt)^k=Nt^k\neq N$. 所以 $|Nt|=h$. 且 $h\mid n$. 如果 $|t|=r$, 则 $(Nt)^r=Nt^r=Ne=N$, 由第四章, 一, 6, $h\mid r$.

29. 证 设群 G 关于子群 $Z(x)$ 的左陪集分解式为 $G=g_1Z(x)\cup g_2Z(x)\cup\cdots\cup g_tZ(x)$, 则
$$\phi:\ g_iZ(x)\to g_ixg_i^{-1},\quad i=1,2,\cdots,t$$
是 $Z(x)$ 的所有左陪集的集合 $S=\{g_iZ(x)\mid i=1,2,\cdots,t\}$ 与 $D=\{y\in G\mid y=gxg^{-1},g\in G\}$ 间的一个一一映射. 事实上:

1) $\forall g_iZ(x)\in S$, $\exists\, g_ixg_i^{-1}\in D$, 使得
$$\phi:\ g_iZ(x)\to g_ixg_i^{-1},\quad i=1,2,\cdots,t.$$
若 $g_iaZ(x)=g_iaZ(x)$, 其中 $a\in Z(x)$,
$$\phi:\ g_iaZ(x)\to g_iax(g_ia)^{-1}=g_iaxa^{-1}g_i^{-1}=g_ixaa^{-1}g_i^{-1}=g_ixg_i^{-1},$$
从而 $\forall g_iZ(x)\in S$, $\exists|\, g_ixg_i^{-1}\in D$, 使得
$$\phi:\ g_iZ(x)\to g_ixg_i^{-1},\quad i=1,2,\cdots,t,$$

即ϕ是映射.

2) $\forall gxg^{-1}\in D, g\in G$,有 $gZ(x)\in S$,即 $gZ(x)=$某 $g_iZ(x)$,使

$$\phi: gZ(x)=g_iZ(x)\to g_ixg_i^{-1},$$

从而ϕ是满射.

3) $\forall g_iZ(x), g_jZ(x)\in S$. 若 $g_ixg_i^{-1}=g_jxg_j^{-1}$,则 $g_j^{-1}g_ix=xg_j^{-1}g_i$,于是 $g_j^{-1}g_i\in Z(x)$,从而 $g_iZ(x)=g_jZ(x)$. 即ϕ是单射.

综上,ϕ是 S 与 D 间的一个一一映射. 所以 D 含元的个数$=S$ 含元的个数 $t=[G:Z(x)]$.

注 由该命题及 Lagrange 定理知,与 $x(\in G)$共轭的元的个数是 G 的阶的因子.

30. 证 $\forall x,y\in G$,规定

$$x\sim y\Leftrightarrow y\text{ 与 }x\text{ 共轭,即 }\exists a\in G\text{,使得 }y=axa^{-1}$$

(见第八章,一,7,1)). 于是共轭关系$\sim$是 G 的元间的一个等价关系. 事实上,$\forall x\in G$,$x=xxx^{-1}$,从而 $x\sim x$,即反射律成立. $\forall x,y\in G$,若 $x\sim y$,则$\exists a\in G$,使得 $y=axa^{-1}$,即 $x=a^{-1}ya$,从而 $y\sim x$,即对称律成立. $\forall x,y,z\in G$,若 $x\sim y$,$y\sim z$,则$\exists a,b\in G$,使得 $y=axa^{-1}$,$z=byb^{-1}$,于是 $z=baxa^{-1}b^{-1}=bax(ba)^{-1}$,从而 $x\sim z$,即推移律成立. 所以共轭关系$\sim$是 G 的元间的一个等价关系. 因此可以利用共轭关系$\sim$将 G 分类,得 $G=D_1\cup D_2\cup\cdots\cup D_r$,其中类 D_i 称为共轭类,$i=1,2,\cdots,r$. 且共轭类 $D_1=\{e\}$(因为与 G 的单位元 e 共轭的元有且只有 e,所以$\{e\}$是一个共轭类). 设 d_i 为 D_i 中的元的个数. 因当 $i\neq j$ 时,$D_i\cap D_j=\varnothing$,故 $p^n=d_1+d_2+\cdots+d_r$,其中 $d_1=1$. 这个等式称为群的类方程. 由上面 29 题知,$d_i\mid p^n$,$i=1,2,\cdots,r$. 因 p 是素数,故每 $d_i=1$ 或 p 的幂. 假设有且只有 $d_1=d_2=\cdots=d_s=1$. 因 $d_1=1$,故 $s\geqslant 1$,于是 $p^n=s+pt$,其中 t 是一个整数. 因 $p\mid p^n$,$p\mid pt$,故 $p\mid s$,又 $s\geqslant 1$,故 $s\geqslant p$,从而至少有 $d_1=d_2=\cdots=d_p=1$,其中素数 $p\geqslant 2$. 由 $d_2=1$ 知 $D_2=\{b\}$,$b\neq e$,且$\forall a\in G$,有 $b=aba^{-1}$,即 $ba=ab$,于是 $b\in Z$. 又有 $e\in Z$. 所以 Z 中至少含有两个元 e 与 b.

31. 证 由上面 30 题,G 的中心至少含有两个元,又 $Z<G$,故$|Z|\,\big|\,|G|=p^2$,从而$|Z|$为 p 或 p^2. 若$|Z|=p$,又因 $Z\lhd G$,故$|G/Z|=\dfrac{p^2}{p}=p$,从而 G/Z 是循环群. 由第八章,四,12 知 G 是交换群. 若$|Z|=p^2$,则$|G|=|Z|$,又 $Z\subset G$,从而 $G=Z$. 所以 G 是交换群.

32. 证 因$|H|=p$,故 $H=(a)=\{a^0=e,a,a^2,\cdots,a^{p-1}\}$是 p 阶循环群. 由 $p\geqslant 2$,故 $a\neq e$. 又因 $H\lhd G$,从而$\forall g\in G$,与 a 共轭的元 $gag^{-1}\in H$,且 $gag^{-1}\neq e$,即与 a 共轭的元的个数最多有 $p-1$ 个. 由上面 29 题,与 a 共轭的元的个数是$|G|=p^n$ 的因子. 因此与 a 共轭的元的个数有且只有一个. 又 a 必与 a 共轭,于是$\forall g\in G$,与 a 共轭的元 $gag^{-1}=a$,即 $ga=ag$. 从而 $a\in Z$. 因为 $Z<G$,所以 $H=(a)\subset Z$.(或:因$\forall a^t\in H$,$\forall g\in G$,都有 $a^tg=a^{t-1}ag=a^{t-1}ga=a^{t-2}aga=a^{t-2}ga^2=\cdots=ga^t$,故 $a^t\in Z$,所以 $H\subset Z$.)

33. 证 对 n 用归纳法. 当 $n=2$ 时,$G=(a)$是 2 阶循环群,且$|a|=2$. 因 p 是素数,$p\mid 2$,故 p 只能是 2,从而 G 中存在阶为 $p=2$ 的元 a.

假定对于 $m<n$,命题成立. 今看 $n(\neq 1)$的情形. 取 $a\in G$,$a\neq e$. 因 G 是有限群,故 a 的阶有限,设$|a|=k$,则 $k\neq 1$. 所以 $k\mid n$.

1) 若 $p\mid k$,则 $a^{\frac{k}{p}}\in G$ 且 $|a^{\frac{k}{p}}|=\dfrac{|a|}{\left(|a|,\dfrac{k}{p}\right)}=\dfrac{k}{\left(k,\dfrac{k}{p}\right)}=\dfrac{k}{\dfrac{k}{p}}=p$,从而 G 中存在阶为 p

的元$a^{\frac{k}{p}}$.

2) 若$p\nmid k$.因G是交换群,故$(a)\lhd G$.从而$G/(a)$是交换商群,且$G/(a)$的阶$m=\frac{|G|}{|(a)|}=\frac{n}{k}<n$.已知$p\mid n=mk$,又$p\nmid k$,$p$是素数,于是$p\mid m$.今有一个有限交换群$G/(a)$,$|G/(a)|=m<n$.$p$是素数,$p\mid m$.由归纳假定,$G/(a)$中存在阶为$p$的元$b(a)$,其中$b\in G$.于是$b^p(a)=(b(a))^p=(a)$,$(a)$是$G/(a)$的单位元.因此$b^p\in(a)$.因$|a|=k$,即$|(a)|=k$,故由第七章,三,1,7),$(b^p)^k=e$,从而$(b^k)^p=e$.由第四章,一,6,$|b^k|\mid p$.因$p$是素数,故$|b^k|=1$或$|b^k|=p$.若$|b^k|=1$,则$b^k=e$,于是$(b(a))^k=b^k(a)=e(a)=(a)$.又$|b(a)|=p$.由第四章,一,6,$p\mid k$.此与假设$p\nmid k$矛盾.因而只能$|b^k|=p$.所以$G$中存在$p$阶元$b^k$.由归纳原理,命题得证.(还可利用下面方法证明$G$中存在$p$阶元.已知$|b(a)|=p$.设$b$在$G$中的阶为$s$,则$(b(a))^s=b^s(a)=e(a)=(a)$.由第四章,一,6,$p\mid s$,于是$\exists$正整数$t$,使得$s=pt$.从而$|b^t|=\frac{|b|}{(|b|,t)}=\frac{s}{(s,t)}=\frac{s}{t}=p$.所以$G$中存在$p$阶元$b^t$.)

34. 证 $\forall x,y\in G$,$x\sim y\Leftrightarrow y$与x共轭,即$\exists a\in G$,使得$y=axa^{-1}$.由上面30题的证明知,共轭关系$\sim$是G的元间的一个等价关系.利用共轭关系$\sim$将G分类,得$G=D_1\cup D_2\cup\cdots\cup D_r$,其中$D_i=\{y\in G\mid y=gx_ig^{-1},g\in G\}$是共轭类,$i=1,2,\cdots,r$.设$d_i$为$D_i$中的元的个数,则$|G|=d_1+d_2+\cdots+d_r$.由上面29题知$d_i=[G:Z(x_i)]$,其中$Z(x_i)$是元$x_i$在$G$内的中心化子,即$Z(x_i)=\{a\in G\mid x_ia=ax_i\}<G$.所以$|G|=[G:Z(x_1)]+[G:Z(x_2)]+\cdots+[G:Z(x_r)]$.我们有下面结论:设$Z$是$G$的中心,则$x\in Z\Leftrightarrow x$所在的共轭类是只含元$x$本身的集$\{x\}$.事实上,($\Rightarrow$) 因$x\in Z$,故$x$所在的共轭类是$\{y\in G\mid y=gxg^{-1},g\in G\}=\{y\in G\mid y=xgg^{-1}=x,g\in G\}=\{x\}$.所以中心$Z$中每一个元$x$自身就构成一个共轭类$\{x\}$.($\Leftarrow$) 因$\{x\}$是只含元$x$的共轭类,故$x=gxg^{-1}$,$\forall g\in G$.从而$xg=gx$,于是$x\in Z$.设$G$的中心$Z$恰含$k(1\leqslant k\leqslant r)$个元,即$Z=\{x_1,x_2,\cdots,x_k\}<G$,则

$$|G|=|Z|+[G:Z(x_{k+1})]+\cdots+[G:Z(x_r)] \quad (*)$$

此即为G的类方程.

1) 如果$k=r$,则$|G|=|Z|$,又$Z\subset G$,从而$G=Z$,即G是交换群.由上面33题知G有q阶子群.

2) 如果$k<r$.

① 若$\exists Z(x_i)(k+1\leqslant i\leqslant r)$,而$|Z(x_i)|=q$,于是$G$中存在$q$阶子群$Z(x_i)$.

② 若$|Z(x_i)|\neq q$,$i=k+1,k+2,\cdots,r$.因$x_i\notin Z$,故$|Z(x_i)|\neq 1$.因$|Z|\geqslant 1$,故$|Z(x_i)|\neq pq$.又$|Z(x_i)|\mid pq$,从而$|Z(x_i)|=p$.于是$[G:Z(x_i)]=\frac{|G|}{|Z(x_i)|}=\frac{pq}{p}=q$.显然$q\mid |G|$.因此由等式($*$),$q\mid |Z|$,而中心$Z$是交换群,由上面33题,$Z$中存在阶为$q$的元$x_j$,当然$x_j$也是$G$中的$q$阶元.所以$G$有$q$阶子群$(x_j)$.

注 该命题说明pq(p与q是互异素数)阶群必有p阶和q阶子群.从而6($=2\times3$)阶群必有2阶和3阶子群(见第七章,四,15).

35. 证一 设$p\mid |G|=n$,p是素数.以满足条件$a_1a_2\cdots a_p=e$的所有p元序列$(a_1,a_2,\cdots,$

a_p)为元素作集 $S=\{(a_1,a_2,\cdots,a_p)\mid a_i\in G,a_1a_2\cdots a_p=e\}$. 规定

$$(a_1,a_2,\cdots,a_p)=(b_1,b_2,\cdots,b_p)\Leftrightarrow a_i=b_i,i=1,2,\cdots,p.$$

1) $\forall(a_1,a_2,\cdots,a_p)\in S$. 因 $a_1a_2\cdots a_p=e$,故 $a_p=(a_1a_2\cdots a_{p-1})^{-1}$,即 a_p 由 $a_1,a_2,\cdots,a_{p-1}$确定. 从而 p 元序列$(a_1,a_2,\cdots,a_p)$由 $p-1$ 个分量可完全确定. 所以集 S 含 n^{p-1}个元.

2) $\forall(a_1,a_2,\cdots,a_p)\in S$,有 $a_1a_2\cdots a_p=a_1(a_2a_3\cdots a_p)=e$,即 a_1 与 $a_2a_3\cdots a_p$ 互为逆元,从而$(a_2a_3\cdots a_p)a_1=e$. 于是$(a_2,a_3,\cdots,a_p,a_1)\in S$. 类似地,有$(a_3,a_4,\cdots,a_p,a_1,a_2),\cdots,(a_p,a_1,a_2,\cdots,a_{p-1})$都$\in S$.

3) 设$(a_1,a_2,\cdots,a_p),(a_2,a_3,\cdots,a_p,a_1),\cdots,(a_p,a_1,a_2,\cdots,a_{p-1})\in S$. 则这 p 个 S 中的元或者都相等,或者互不相等. 即或者它们是同一个序列,或者它们是 p 个不同的序列. 事实上,只需证明,若这 p 个 S 中的元有两个相等,则这 p 个 S 中的元都相等.

设$(a_1,a_2,\cdots,a_p)=(a_{i+1},a_{i+2},\cdots,a_{i+p})$(其中 $1\leqslant i<p$. 若 $i+k>p$. 则设 $i+k=pq+r$,$0\leqslant r<p$,有 $a_{i+k}=a_{r+1},k=1,2,\cdots,p$). 则 $a_1=a_{i+1},a_2=a_{i+2},\cdots,a_p=a_{i+p}$. 于是对 i 来说,有 $a_i=a_{i+i}=a_{2i},a_{2i}=a_{i+2i}=a_{3i},\cdots,a_{(p-1)i}=a_{pi}$. 即 $a_i=a_{2i}=a_{3i}=\cdots=a_{pi}$. 设 $i=pq_1+r_1,2i=pq_2+r_2,\cdots,pi=pq_p+r_p,0\leqslant r_l<p,l=1,2,\cdots,p$. 则 $a_i=a_{r_1+1},a_{2i}=a_{r_2+1},\cdots,a_{pi}=a_{r_p+1}$,从而,$a_{r_1+1}=a_{r_2+1}=\cdots=a_{r_p+1}$. 且 $r_1+1,r_2+1,\cdots,r_p+1$ 互不相等. 因为假定 $r_s+1=r_t+1$,其中 $s\neq t,s,t=1,2,\cdots,p$. 又 $si=pq_s+r_s$, $ti=pq_t+r_t$, 于是 $si-ti=p(q_s-q_t)$,即 $p\mid si-ti=(s-t)i$,但 $1\leqslant i<p$,p 是素数,从而$(p,i)=1$,因此 $p\mid s-t$,又 $s,t=1,2,\cdots,p$,即$|s-t|<p$,可见 $s-t=0$,即 $s=t$,发生矛盾. 所以 $r_1+1,r_2+1,\cdots,r_p+1$ 互不相等. 又 $0\leqslant r_l<p,l=1,2\cdots,p$,从而 $r_1+1,r_2+1,\cdots,r_p+1$ 即为 p 个数 $1,2,\cdots,p$,因此 $a_{r_1+1},a_{r_2+1},\cdots,a_{r_p+1}$即为 $a_1,a_2,\cdots,a_p$,于是 $a_1=a_2=\cdots=a_p$. 即 p 个 S 中的元$(a_1,a_2,\cdots,a_p),(a_2,a_3,\cdots,a_p,a_1),\cdots,(a_p,a_1,a_2,\cdots,a_{p-1})$都相等,实际上是同一个元.

4) 规定$(a_1,a_2,\cdots,a_p),(b_1,b_2,\cdots,b_p)\in S,(a_1,a_2,\cdots,a_p)\sim(b_1,b_2,\cdots,b_p)\Leftrightarrow b_1,b_2,\cdots,b_p$ 是 3)中 p 个序列之一. 易证$\sim$是 S 的元间的一个等价关系. 利用此等价关系$\sim$对 S 进行分类,得 $S=C_1\cup C_2\cup\cdots\cup C_q$,其中必有一个类设为 C_1 只含 1 个元$(\overbrace{e,e,\cdots,e}^{p个})$,即 $C_1=\{(\overbrace{e,e,\cdots,e}^{p个})\}$. 我们有下面的类方程

$$n^{p-1}=1+C_2\text{ 中含元的个数}+\cdots+C_q\text{ 中含元的个数}.$$

由 3)知每一个类 $C_i(i=1,2,\cdots,q)$中的元的个数或为 1 或为 p. 因 $p\mid n$,故 $p\mid n^{p-1}$,p 是素数,$p\geqslant 2$,从而 $C_2,C_3,\cdots,C_q$ 中必至少有一个类含且只含 1 个元. 不妨设 $C_2=\{(\overbrace{a,a,\cdots,a}^{p个})\}$. 因$(\overbrace{a,a,\cdots,a}^{p个})\in S$,故$\overbrace{aa\cdots a}^{p个}=a^p=e$,又 p 是素数,$a\neq e$,从而$|a|=p$. 所以 G 中有 p 阶元 a.

证二 设 p 是素数,$p\mid |G|=n$,则$\exists$正整数 m,使得 $n=mp$. 对 m 作归纳法.

1) 当 $m=1$ 时,G 是 p 阶循环群,从而 $G=(a)$,于是$|a|=p$. 所以 G 中有 p 阶元 a.

2) 假定 $k<m$ 时,命题成立. 今看 $n=mp$ 时. 分两种情形讨论:

① 设 G 有真子群 H 使 $p\nmid[G:H]$.

因 $p\mid |G|=|H|[G:H]$,p 是素数,故 $p\mid |H|$. 于是$\exists$正整数 k,使得$|H|=kp$. 因$|H|=$

$kp<|G|=mp$,故 $k<m$. 由归纳假定,H 含有 p 阶元 a,从而 G 也含有 p 阶元 a,所以命题成立.

② 设 G 的任一真子群 H 都使 $p\mid[G:H]$.

由上面 34 题的证明知 G 有类方程

$$|G|=|Z|+[G:Z(a_1)]+\cdots+[G:Z(a_t)],$$

其中 Z 是 G 的中心,$Z(a_i)$ 是元 a_i 在 G 内的中心化子,即 $Z(a_i)=\{x\in G\mid xa_i=a_ix\}$. 因 $|Z(a_i)|\neq1$,$|Z(a_i)|\neq|G|$,故 $Z(a_i)$ 是 G 的真子群. 由 $p\mid|G|$,$p\mid[G:Z(a_i)]$,$i=1,2,\cdots,t$,有 $p\mid|Z|$. 又中心 Z 是交换群,从而由上面 33 题,在 Z 中存在 p 阶元 a,当然 a 也是 G 中的 p 阶元,所以命题成立.

注 1) 该命题是上面 33 题与 34 题的推广.

2) 证一见 Mckay J. H. Another proof of Cauchy's group theorem, American Mathematical Monthly, 1956, 66:119.

36. 证一 因 p,q 是素数,且 $p\mid|G|$,$q\mid|G|$,故由上面 35 题,G 中存在 p 阶元 a 和 q 阶元 b. 因 p,q 互异,故 $(p,q)=1$. 又 G 是交换群,从而 $ab=ba$,于是由第七章,二,8,$|ab|=pq$. 所以 $G=(ab)$ 是循环群.

证二 要证 G 是循环群,只需证明 G 中有 pq 阶元. 我们知道,G 的元的阶整除 $|G|=pq$. 因 p,q 是互异素数,故 G 的元的阶或为 1,或为 p,或为 q,或为 pq. 又因 $|G|=pq$,故 $|G|\neq1$,从而 $\exists a\in G,a\neq e$. 若 $|a|=pq$,则 $G=(a)$ 是循环群,命题得证. 若 $|a|\neq pq$. 不妨设 $|a|=p$. 令 $H=(a)$. 因 G 是交换群,故 H 是 G 的 p 阶不变子群,从而 G/H 是商群. $|G/H|=\frac{|G|}{|H|}=\frac{pq}{p}=q$. 因 q 是素数,故 $G/H=(bH)$ 是 q 阶循环群. 于是 $(bH)^q=H$,即 $b^qH=H$,从而 $b^q\in H$. 则 $|b|\neq p$. 事实上,假设 $|b|=p$,则 $b^p=e\in H$,已知 $b^q\in H$. 由 $(p,q)=1$,$\exists$ 整数 s,t,使得 $ps+qt=1$,于是 $b=b^{ps+qt}=(b^p)^s(b^q)^t=(b^q)^t\in H$,因此 $bH=H$. 所以 $G/H=(bH)=(H)=\{H\}$ 是 1 阶群,此与 $|G/H|=q$ 矛盾. 所以 $|b|\neq p$. 又 $b\neq e$. 不然,若 $b=e$,则 $G/H=(bH)=(H)=\{H\}$ 是 1 阶群,也产生矛盾. 由上可见 $|b|=pq$ 或 q. 若 $|b|=pq$,则 $G=(b)$ 为循环群. 若 $|b|=q$,因 $(p,q)=1$,又 G 是交换群,$ab=ba$,故由第七章,二,8,$|ab|=|a||b|=pq$. 所以 $G=(ab)$ 是循环群.

注 1) 在证二中,还可如下证明 $|b|\neq p$. 事实上,假设 $|b|=p$,则 $(bH)^p=b^pH=eH=H$,又 $|bH|=q$,从而 $q\mid p$. 发生矛盾. 所以 $|b|\neq p$.

2) 该命题说明 6 阶,10 阶,14 阶,15 阶,21 阶等有限交换群都是循环群.

37. 证一 (反证法)若 pq 阶群 G 有两个不同的 q 阶子群 H_1 与 H_2. 则由第八章,四,5,乘积 H_1H_2 中含元的个数 $|H_1H_2|=\frac{|H_1|\cdot|H_2|}{|H_1\cap H_2|}\leqslant|G|=pq$. 因 q 是素数,故 H_1,H_2 都是循环群,且 H_i 中除单位元外,每个元都是生成元,$i=1,2$. 又 $H_1\neq H_2$,则必有 $H_1\cap H_2=\{e\}$. 否则,若 $\exists a\in H_1\cap H_2,a\neq e$,则 $a\in H_1$ 且 $a\in H_2$,于是 $(a)=H_1=H_2$,此与 $H_1\neq H_2$ 矛盾. 所以 $H_1\cap H_2=\{e\}$. 于是 $|H_1H_2|=|H_1|\cdot|H_2|=q^2\leqslant pq$. 此与 $q>p$ 矛盾. 所以 pq 阶群不能有两个不同的 q 阶子群.

证二 (反证法)设 H_1,H_2 是 G 的两个不同的 q 阶子群. 因 q 是素数,故 $H_1=(a)$,H_2

$=(b)$都是循环群. 又 $H_1\cap H_2$ 是 H_1 的子群，从而 $|H_1\cap H_2|\,\big|\,|H_1|=q$，从而 $|H_1\cap H_2|=1$ 或 q. 若 $|H_1\cap H_2|=q$，则 $|H_1\cap H_2|=|H_1|=|H_2|$，从而 $H_1\cap H_2=H_1$，$H_1\cap H_2=H_2$，即 $H_1=H_2$. 矛盾. 所以 $|H_1\cap H_2|=1$，即 $H_1\cap H_2=\{e\}$. 因 $H_1=(a)=\{a^0=e,a,a^2,\cdots,a^{q-1}\}$，$H_2=(b)=\{b^0=e,b,b^2,\cdots,b^{q-1}\}$，故乘积 $H_1H_2=\{a^ib^j\mid i,j=0,1,2,\cdots,q-1\}\subset G$. 则 H_1H_2 中的 q^2 个元各不相同. 事实上，若有 $a^ib^j=a^kb^l$，$i\neq k$ 或 $j\neq l$，$0\leqslant i,j,k,l\leqslant q-1$，则 $a^{i-k}=b^{l-j}\in H_1\cap H_2=\{e\}$，此与 $i\neq k$ 或 $j\neq l$ 矛盾. 因而 H_1H_2 恰含 q^2 个互不相同的元. 已知 $q>p$，就得出 H_1H_2 中元的个数 $q^2>pq=|G|$，此与 $H_1H_2\subset G$ 矛盾. 所以 G 不可能有两个不同的 q 阶子群.

38. 证 由上面 37 题知，pq 阶群 G 不能有两个不同的 q 阶子群. 由第八章，三，2，6)，G 的 q 阶子群是不变子群.

39. 证 1) 先证 $H=\{x\in G\,|\,x^p=e\}<G$. 因方程 $x^p=e$ 在 G 内恰有 p 个解，p 是素数，$p\geqslant 2$，故方程 $x^p=e$ 在 G 内至少有两个解. 于是 $\exists\, a\in G$，$a\neq e$，使得 $a^p=e$，即 $a\in H$. 又 $(a^0)^p=e^p=e$，$(a^2)^p=(a^p)^2=e^2=e$，$\cdots$，$(a^{p-1})^p=(a^p)^{p-1}=e^{p-1}=e$. 于是 $a^0=e,a,a^2,\cdots,a^{p-1}\in H$. 因 $a^p=e$，故 $|a|\,\big|\,p$，又 p 是素数，$a\neq e$，从而 $|a|=p$. 因此 $(a)=\{a^0=e,a,a^2,\cdots,a^{p-1}\}$是一个 p 阶循环群且$(a)\subset H$，又 H 也含 p 个元，所以 $H=(a)<G$.

2) 再证 $H=(a)\lhd G$. $\forall\, g\in G$，$\forall\, a^\lambda\in(a)=H$，$\lambda=0,1,2,\cdots,p-1$. 当 $\lambda=0$ 时，显然有 $ga^\lambda g^{-1}=ga^0g^{-1}=geg^{-1}=e\in(a)=H$. 当 $0<\lambda\leqslant p-1$ 时，因 $|ga^\lambda g^{-1}|=|a^\lambda gg^{-1}|=|a^\lambda|=\dfrac{|a|}{(\lambda,|a|)}=\dfrac{p}{(\lambda,p)}=p$，故 $(ga^\lambda g^{-1})^p=e$，从而 $ga^\lambda g^{-1}\in H$. 所以 $H\lhd G$.（或用下面方法证明 $H\lhd G$. $\forall\, g\in G$，$\forall\, x\in H$，$(gxg^{-1})^p=\overbrace{(gxg^{-1})(gxg^{-1})\cdots(gxg^{-1})}^{p\text{个}}=gx^pg^{-1}=geg^{-1}=e$，从而 $gxg^{-1}\in H$. 所以 $H\lhd G$.）

40. 1) 正确. **证** 因ϕ是群 G 到 $\overline{G}$ 的一个同态映射，故ϕ是群 G 到 $\overline{G}$ 的象$\phi(G)$的一个同态满射. 又 G 在同态满射ϕ下的象$\phi(G)$是 $\overline{G}$ 的一个子群①，从而ϕ是群 G 到 $\overline{G}$ 的一个子群 $\overline{G}_1=\phi(G)$的同态满射. 反之，命题显然成立.

2) 正确. **证** 设 $A\overset{\phi_1}{\cong}B'$，$B\overset{\phi_2}{\cong}A'$. 因 B'是 B 的真子群，故 B'在ϕ_2 下的象 A''是 A'的子群，当然 A''是 A 的真子群，且 $B'\cong A''$. 所以 $A\cong A''$.

同理，因 A'是 A 的真子群，故 A'在ϕ_1 下的象 B''是 B'的子群，当然 B''是 B 的真子群，且 $A'\cong B''$. 所以 $B\cong B''$.

3) 不正确. $\phi(H_1)$，$\phi(H_2)$是 $\overline{G}$ 的子群②，但未必$\phi(H_1)\neq\phi(H_2)$. 例，设 G 是整数加群，$\overline{G}=(a)$是 6 阶循环群. $\phi:n\rightarrow a^n$ 是 G 到 $\overline{G}$ 的同态满射. G 有无限多个子群. 事实上，任取整数 n，G 就有一个以 n 为生成元的子群 $H=(n)$. 并且，若 $m\neq\pm n$，则子群 $H'=(m)\neq H$，从而 G 有无限多个子群. 而 $\overline{G}=(a)$，$|a|=6$. 因 6 有且只有因子 1，2，3，6，故 $\overline{G}$ 有且只有 4 个子群，即(e)，$(a)=\overline{G}$，$(a^2)=\{e,a^2,a^4\}$，$(a^3)=\{e,a^3\}$. 但 $G\overset{\phi}{\sim}\overline{G}$，从而存在 G 的不同子群 H_1，H_2，使$\phi(H_1)=\phi(H_2)$. 事实上，取 $H_1=(4)=\{4k\,|\,k$ 是整数$\}$，$H_2=(10)=\{10k\,|\,k$ 是

① ② 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 77. 定理 3.

整数$\}$，这是两个不同的G的子群．而$\phi(H_1)=\{e,a^4,a^2\}$，$\phi(H_2)=\{e,a^4,a^2\}$，因此$\phi(H_1)=\phi(H_2)$．所以存在G的不同子群H_1,H_2，使$\phi(H_1)=\phi(H_2)$．

4）　正确．**证**　$\forall\ \overline{b}\in\overline{B}$，$\exists\, b\in B$，使$\phi: b\to\overline{b}$．又$B\subset A$，于是$b\in A$，因此$\phi(b)=\overline{b}\in\overline{A}$，所以$\overline{B}\subset\overline{A}$．

5）　正确．**证**　由同态基本定理，$\ker\phi\lhd G$，$\ker\psi\lhd G$，且$G/\ker\phi\cong H$，$G/\ker\psi\cong K$．又$G/\ker\phi=G/\ker\psi$，所以$H\cong K$．

6）　正确．**证一**　因$G=(g)$是循环群，即G是交换群，故$H_1\lhd G$，$H_2\lhd G$．由第八章，二，10，G/H_1，G/H_2是循环群．$|H_1|=|g^s|=\dfrac{st}{(s,st)}=\dfrac{st}{s}=t$，$|H_2|=|g^t|=\dfrac{st}{(t,st)}=\dfrac{st}{t}=s$．且$|G/H_1|=\dfrac{|G|}{|H_1|}=\dfrac{st}{t}=s$，$|G/H_2|=\dfrac{|G|}{|H_2|}=\dfrac{st}{s}=t$．由第八章，二，9，$G/H_1\sim H_2$，$G/H_2\sim H_1$．又因$|G/H_1|=|H_2|=s$，$|G/H_2|=|H_1|=t$，故$G/H_1\cong H_2$，$G/H_2\cong H_1$．

证二　要证$G/H_1\cong H_2$，由同态基本定理，只需证$G\overset{\phi}{\sim}H_2$，$H_1=\ker\phi$．因$|G|=|g|=st$，$|H_2|=|g^t|=\dfrac{st}{(t,st)}=\dfrac{st}{t}=s$，即$|H_2|\,\big|\,|G|$，故由第八章，二，9知，$\phi: g^k\to(g^t)^k$是$G=(g)$到$H_2=(g^t)$的一个同态满射，即$G\overset{\phi}{\sim}H_2$．下面证明$\ker\phi=H_1=(g^s)$．事实上，$\forall\, x\in\ker\phi$，$x\in G$，可设$x=g^r$，$\phi(x)=\phi(g^r)=(g^t)^r=g^{tr}$，又$\phi(x)=e$，从而$g^{tr}=e$．于是$|g|=st\,\big|\,tr$，因$t\neq 0$，故$s\,\big|\,r$，即$\exists$整数$q$，使得$r=sq$．因此$x=g^r=g^{sq}=(g^s)^q\in(g^s)=H_1$，从而$\ker\phi\subset H_1$．反之，$\forall\, x\in H_1=(g^s)$，可设$x=(g^s)^l=g^{sl}$，因此$\phi(x)=\phi(g^{sl})=(g^t)^{sl}=(g^{st})^l=e^l=e$，于是$x\in\ker\phi$，从而$H_1\subset\ker\phi$．所以$H_1=\ker\phi$．由同态基本定理，$H_1\lhd G$且$G/H_1\cong H_2$．同理，$H_2\lhd G$，$G/H_2\cong H_1$．

证三　因G是循环群，即G是交换群，故$H_1\lhd G$，$H_2\lhd G$．又$|H_1|=|g^s|=\dfrac{st}{(s,st)}=\dfrac{st}{s}=t$，$|H_2|=|g^t|=\dfrac{st}{(t,st)}=\dfrac{st}{t}=s$．$|G/H_1|=\dfrac{|G|}{|H_1|}=\dfrac{st}{t}=s$，从而$G/H_1=\{H_1g^0,H_1g,H_1g^2,\cdots,H_1g^{s-1}\}$，$H_2=(g^t)=\{(g^t)^0,g^t,(g^t)^2,\cdots,(g^t)^{s-1}\}$．则$\phi: H_1g^i\to(g^t)^i\ (0\leqslant i\leqslant s-1)$是$G/H_1$与$H_2$间的一个同构映射．事实上：

①　$\forall\, H_1g^i\in G/H_1$，$0\leqslant i\leqslant s-1$，$\exists\,\big|\,(g^t)^i\in H_2$，使得$\phi: H_1g^i\to(g^t)^i$．所以$\phi$是映射．

②　$\forall\,(g^t)^i\in H_2$，$0\leqslant i\leqslant s-1$，$\exists\, H_1g^i\in G/H_1$，使得$\phi: H_1g^i\to(g^t)^i$．所以$\phi$是满射．

③　$\forall\, H_1g^i,H_1g^j\in G/H_1$，$0\leqslant i,j\leqslant s-1$．若$(g^t)^i=(g^t)^j$，$0\leqslant i,j\leqslant s-1$，则$i=j$，从而$H_1g^i=H_1g^j$．所以$\phi$是单射．

④　$\forall\, H_1g^i,H_1g^j\in G/H_1$，$0\leqslant i,j\leqslant s-1$．$\phi: H_1g^i\to(g^t)^i$，$H_1g^j\to(g^t)^j$，有

$$(H_1g^i)(H_1g^j)=H_1g^{i+j}\to(g^t)^{i+j}=g^{ti+tj}=(g^t)^i(g^t)^j,$$

所以ϕ是同构映射．于是$G/H_1\overset{\phi}{\cong}H_2$．

类似地可证$G/H_2\cong H_1$．

41. 解　1）　$\ker\phi=\{2q\,|\,q\in\mathbb{Z}\}$．

2）　$\ker\phi=\{1\}$．

3）　$\ker\phi=\{1,-1\}$．

4）　$\ker\phi=\{1,-1\}$．

5) $\ker\phi=\{4q\,|\,q\in\mathbb{Z}\}$.

6) $\ker\phi=\{nq\,|\,q\in\mathbb{Z}\}=(n)$.

7) $\ker\phi=\{[0],[2],[4],[6]\}$.

8) $\ker\phi=\{e,a^2,a^4\}=(a^2)$.

9) $\ker\phi=\{[0],[4],[8]\}$.

10) $\ker\phi=G$.

11) $\ker\phi=\left\{A\in GL_n(\mathbb{R})\,\middle|\,|A|=1\right\}$(第五章,二,6,注 3)).

12) 当$|a|=\infty$时,$\ker\phi=\{0\}$. 当$|a|$有限时,设$|a|=m$,则 $\ker\phi=\left\{mq\,\middle|\,q\in\mathbb{Z}\right\}=(m)$.

13) $\ker\phi=\{x\in G\,|\,x^k=e\}$.

14) $\ker\phi=\left\{\frac{q}{p}\,\middle|\,p,q\text{ 是奇数}\right\}$.

15) $\ker\phi=\left\{A\in G\,\middle|\,|A|=\frac{q}{p},p,q\in\mathbb{Z},p,q\text{ 是奇数}\right\}$.

16) $\ker\phi=\{\tau_{1b}\,|\,\forall x\in\mathbb{R},x^{\tau_{1b}}=x+b,b\in\mathbb{R}\}$.

17) $\ker\phi=\{3^n\,|\,n\in\mathbb{Z}\}$.

42. 证 $\forall\bar{a}\in\bar{G}$,因ϕ是 G 到 $\bar{G}$ 的满射,故$\exists a\in G$,使得$\bar{a}=\phi(a)$. 因 $a\in G=(S)$,故 a 可表为$a=a_1^{k_1}a_2^{k_2}\cdots a_n^{k_n}$,其中 $a_i\in S,k_i=\pm1,n$ 是正整数. 从而 $\bar{a}=\phi(a)=\phi(a_1^{k_1}a_2^{k_2}\cdots a_n^{k_n})=\phi(a_1)^{k_1}\phi(a_2)^{k_2}\cdots\phi(a_n)^{k_n}$,其中$\phi(a_i)\in\phi(S),k_i=\pm1,n$ 是正整数. 因此 $\bar{G}\subset(\phi(S))$. 反之,因ϕ是 G 到 $\bar{G}$ 的映射,故$\phi(S)\subset\bar{G}$. 又 $\bar{G}$ 是群,从而$(\phi(S))\subset\bar{G}$. 所以$(\phi(S))=\bar{G}$.

43. 证 因 $H\lhd G$,故 G/H 是商群. $\forall g\in G$,有 $Hg\in G/H$. 且$|Hg|\,\big|\,|G/H|=m$. 又 G/H 的单位元是 H,从而由第七章,三,1,7),$(Hg)^m=H$,即 $Hg^m=H$. 所以 $g^m\in H$.

注 1) 见第八章,四,25 的证明.

2) "$H\lhd G$"改为"$H<G$",命题不成立. 例,$H=\{(1),(12)\}<S_3$,$[S_3:H]=3$,但 $(13)^3=(13)\overline{\in}H$.

44. 证 (反证法)设$[G:H]=m$. 因 G 是交换群,故 $H\lhd G$. $\forall x\in G$,$\frac{x}{m}$也是有理数,因而$\frac{x}{m}\in G$. 由上面 43 题,$m\left(\frac{x}{m}\right)\in H$,即 $x\in H$,从而 $G\subset H$. 又 $H\subset G$,于是 $H=G$. 此与已知 $H\neq G$ 矛盾. 所以$[G:H]=\infty$.

注 见第八章,四,26.

45. 证 (反证法)设$[G:H]=m$. 因 G 是交换群,故 $H\lhd G$. $\forall x\in G$,因 x 是复数,故$\sqrt[m]{x}$也是复数,即$\sqrt[m]{x}\in G$. 由上面 43 题,$(\sqrt[m]{x})^m\in H$,即 $x\in H$,从而 $G\subset H$,又 $H\subset G$,于是 $H=G$. 此与已知 $H\neq G$ 矛盾. 所以$[G:H]=\infty$.

46. 证一 因 $N\lhd G,N\subset H<G$,故由第八章,三,2,5),$N\lhd H$. 从而 H/N 是商群. 因 $N\subset H\lhd G$,故由第八章,三,14,2),$H/N\lhd G/N$. 从而$(G/N)/(H/N)$是商群. 又$\phi:a\to aN$ 是G 到G/N 的一个同态满射①. 且 H 是 H/N 在ϕ下的逆象. 事实上,$\forall h\in H$,$\phi(h)=hN\in H/N$,从而 $h\in\phi^{-1}(H/N)$,即 $H\subset\phi^{-1}(H/N)$;反之,$\forall a\in\phi^{-1}(H/N)$,$\phi(a)\in H/N$,可设$\phi(a)=hN$,其中 $h\in H$,又$\phi(a)=aN$,于是 $aN=hN$,因此 $h^{-1}a\in N$,可设$h^{-1}a=n\in N$,从而

① 张禾瑞. 近世代数基础. 北京:高等教育出版社,1978. 75. 定理 1.

$a=hn\in H$，即$\phi^{-1}(H/N)\subset H$. 所以 $H=\phi^{-1}(H/N)$. 由第八章，二，8，$G/H\cong(G/N)/(H/N)$.

证二 $\forall a\in G$，$\phi: aN\to aH$ 是 G/N 到 G/H 的同态满射. 事实上，1) $\forall aN\in G/N$，$\exists aH\in G/H$，使得$\phi(aN)=aH$. 若 $aN=bN$，则 $b^{-1}a\in N\subset H$，于是 $aH=bH$，从而 $\exists | aH\in G/H$，使得$\phi(aN)=aH$；2) $\forall aH\in G/H$，$\exists aN\in G/N$，使得$\phi(aN)=aH$；3) $\forall aN, bN\in G/N$，$\phi(aN\cdot bN)=\phi((ab)N)=(ab)H=aH\cdot bH=\phi(aN)\cdot\phi(bN)$. 所以 $G/N\overset{\phi}{\sim}G/H$. 因 $N\lhd G$，$N\subset H<G$，故由第八章，三，2，5)，$N\lhd H$，从而 H/N 是商群. 且 $\ker\phi=H/N$. 事实上：$\forall aN\in\ker\phi$，$\phi(aN)=H$，又$\phi(aN)=aH$，于是 $H=aH$，从而 $a\in H$，因此 $aN\in H/N$，即 $\ker\phi\subset H/N$；反之，$\forall hN\in H/N$，其中 $h\in H$，$\phi(hN)=hH=H$，因此 $hN\in\ker\phi$，即 $H/N\subset\ker\phi$. 所以 $\ker\phi=H/N$. 由同态基本定理，$\ker\phi=H/N\lhd G/N$ 且 $(G/N)/(H/N)\cong G/H$.

例 设 G 是整数加群 $\mathbb{Z}$. $N=(6)=\{\cdots,-12,-6,0,6,12,\cdots\}$. $H=(3)=\{\cdots,-12,-9,-6,-3,0,3,6,9,12,\cdots\}$. 则 $\mathbb{Z}/(6)=\mathbb{Z}_6=\{[0],[1],[2],\cdots,[5]\}$. $\mathbb{Z}/(3)=\mathbb{Z}_3=\{[0],[1],[2]\}$. $(3)/(6)=\{0+(6),3+(6)\}=\{[0],[3]\}$. $(\mathbb{Z}/(6))/((3)/(6))=\{[0]+(3)/(6),[1]+(3)/(6),[2]+(3)/(6)\}=\{\{[0],[3]\},\{[1],[4]\},\{[2],[5]\}\}$. 由上命题知，$(\mathbb{Z}/(6))/((3)/(6))\cong\mathbb{Z}/(3)$.

47. 证 因 $N\lhd G$，$H\lhd G$，故由第八章，二，4，注 10)，$NH\lhd G$. 又 $N\subset NH$，从而由上面 46 题，$G/NH\cong(G/N)/(NH/N)$.

48. 证一 因 $N\lhd G$，$H<G$，故由第八章，二，4，$NH<G$. 又 $N\subset NH<G$，由第八章，三，2，5)，$N\lhd NH$，从而 NH/N 是商群. $\forall h\in H$，$\phi: h\to Nh$ 是 H 到 NH/N 的一个同态满射. 事实上，1) $\forall h\in H$，$\exists | Nh\in NH/N$，使得$\phi(h)=Nh$. 2) $\forall Nnh\in NH/N$，其中 $n\in N$，$h\in H$. 从而 $Nnh=Nh$. 于是 $\exists h\in H$，使得$\phi(h)=Nh=Nnh$. 3) $\forall h,h'\in H$，$\phi(hh')=N(hh')=Nh\cdot Nh'=\phi(h)\phi(h')$. 所以 $H\overset{\phi}{\sim}NH/N$. 下面证明 $\ker\phi=N\cap H$. 事实上，$a\in\ker\phi$，$a\in H\Leftrightarrow\phi(a)=Na=N\Leftrightarrow a\in N$，又 $a\in H\Leftrightarrow a\in N\cap H$. 所以 $\ker\phi=N\cap H$. 由同态基本定理，$N\cap H\lhd H$ 且 $H/(N\cap H)\cong NH/N$.

证二 因 $N\lhd G$，$H<G$，故由第八章，二，2，注 2)，$N\cap H\lhd H$. 由第八章，二，4，$NH<G$. 又 $N\subset NH<G$，由第八章，三，2，5)，$N\lhd NH$. 所以 $H/(N\cap H)$ 与 NH/N 都是商群. $\forall(N\cap H)a\in H/(N\cap H)$，其中 $a\in H$，$\phi:(N\cap H)a\to Na$ 是 $H/(N\cap H)$ 到 NH/N 的同构映射. 事实上，1) $\forall(N\cap H)a\in H/(N\cap H)$，其中 $a\in H$，$\exists Na\in NH/N$，使得 $\phi((N\cap H)a)=Na$. 若$(N\cap H)a=(N\cap H)b$，其中，$a,b\in H$，则 $ab^{-1}\in N\cap H$，于是 $ab^{-1}\in N$，从而 $Na=Nb$. 因此 $\exists | Na\in NH/N$，使得$\phi((N\cap H)a)=Na$. 2) $\forall Nnh\in NH/N$，其中 $n\in N$，$h\in H$，于是 $Nnh=Nh$. 因此 $\exists(N\cap H)h\in H/(N\cap H)$，使得$\phi((N\cap H)h)=Nh=Nnh$. 3) $\forall(N\cap H)a,(N\cap H)b\in H(N\cap H)$，其中 $a,b\in H$. 若 $Na=Nb$，则 $ab^{-1}\in N$. 又 $ab^{-1}\in H$，于是 $ab^{-1}\in N\cap H$. 因此，$(N\cap H)a=((N\cap H)b$. 4) $\forall(N\cap H)a,(N\cap H)b\in H/(N\cap H)$，其中 $a,b\in H$. $\phi\big((N\cap H)a\cdot(N\cap H)b\big)=\phi\big((N\cap H)ab\big)=Nab=Na\cdot Nb=\phi\big((N\cap H)a\big)\cdot\phi\big((N\cap H)b\big)$. 所以，$H/(N\cap H)\overset{\phi}{\cong}NH/N$.（在证明了$\phi$是群 $H/(N\cap H)$到群 NH/N 的同态满射以后，再证明$\ker\phi=\{N\cap H\}$，则由第八章，三，13 知，ϕ是

单射，于是也可得 $H/(N\cap H)\overset{\phi}{\cong} NH/N$. 下面证明 $\ker\phi=\{N\cap H\}$. $\forall (N\cap H)h\in\ker\phi$, $h\in H$，有 $\phi((N\cap H)h)=Nh=N$，从而 $h\in N$，又 $h\in H$，于是 $h\in N\cap H$. 即 $(N\cap H)h=N\cap H$. 所以 $\ker\phi=\{N\cap H\}$.）

证三 $\forall a\in G$，$\phi: a\to Na$ 是 G 到 G/N 的一个同态满射，且 $\ker\phi=N$. 因 $H<G$，故 H 在 ϕ 下的象 $\overline{H}<G/N$. 由第八章，三，14，1)，$\overline{H}=H/N$. 因此 $H\overset{\phi'}{\sim}H/N$ 且 $\phi': h\to Nh(h\in H)$ 是 H 到 H/N 的一个同态满射. $\ker\phi'=N\cap H$. 事实上，$h\in\ker\phi'$，$h\in H\Leftrightarrow \phi'(h)=Nh=N\Leftrightarrow h\in N$. 又 $h\in H\Leftrightarrow h\in N\cap H$. 所以，$\ker\phi'=N\cap H$. 由同态基本定理，$N\cap H\lhd H$ 且 $H/(N\cap H)\cong H/N$. 由第八章，二，7，注 2)，H/N 在 ϕ 下的逆象是 $H\ker\phi=HN$. 因 $HN<G$，故由第八章，二，4，注 4)，$HN=NH$，即 H/N 在 ϕ 下的逆象是 NH. 于是，$\forall nh\in NH$，其中 $n\in N$，$h\in H$，$\psi: nh\to Nh$ 是 NH 到 H/N 的一个同态满射，且 $\ker\psi=N$. 事实上，$\forall nh\in\ker\psi$，其中 $n\in N$，$h\in H$，$\psi(nh)=Nh=N$，于是 $h\in N$，即 $nh\in N$，因此 $\ker\psi\subset N$；反之，$\forall n\in N$，$\psi(n)=\psi(ne)=Ne=N$，于是 $n\in\ker\psi$. 所以 $\ker\psi=N$. 由同态基本定理，$NH/N\cong H/N$. 即 $H/N\cong NH/N$. 由同构的传递性，$H/(N\cap H)\cong NH/N$.

注 1) 该命题是一个很有用的同构定理. 见下例.

例 设 $G=(a)$ 是无限循环群，n,m 是正整数，则 $N=(a^n)\lhd(a)$，$H=(a^m)<(a)$. 由该命题知 $(a^m)/((a^n)\cap(a^m))\cong(a^n)(a^m)/(a^n)$. 设 $l=[n,m]$，由第七章，四，10，$(a^n)\cap(a^m)=(a^l)$. 设 $d=(n,m)$，则 $(a^n)(a^m)=(a^d)$. 事实上，$\forall (a^n)^s(a^m)^t\in(a^n)(a^m)$. 因 $(a^n)^s(a^m)^t=a^{ns+mt}$，又 $d\,|\,n$，$d\,|\,m$，即 $d\,|\,ns+mt$，于是 $\exists q\in\mathbb{Z}$，使得 $ns+mt=dq$，故 $(a^n)^s(a^m)^t=a^{dq}=(a^d)^q\in(a^d)$. 从而 $(a^n)(a^m)\subset(a^d)$；反之，$\forall (a^d)^r\in(a^d)$，因 $d=(n,m)$，故 $\exists u,v\in\mathbb{Z}$，使得 $nu+mv=d$. 于是 $(a^d)^r=a^{nur+mvr}=(a^n)^{ur}(a^m)^{vr}\in(a^n)(a^m)$. 从而 $(a^d)\subset(a^n)(a^m)$. 所以 $(a^n)(a^m)=(a^d)$. 因此 $(a^m)/(a^l)\cong(a^d)/(a^n)$，其中 $l=[n,m]$，$d=(n,m)$.

例 设 $N=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}\lhd S_4$（见第八章，二，5），$H=S_3=\{(1),(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2)\}<S_4$. 由该命题知 $NS_3/N\cong S_3/(N\cap S_3)$. 但 $N\cap S_3=\{(1)\}$，从而 $NS_3/N\cong S_3/\{(1)\}\cong S_3$. 因 $|S_3|=6$，故 $|NS_3/N|=6$，于是 $|NS_3|=|N|[NS_3:N]=4\times6=24=|S_4|$. 又 $NS_3\subset S_4$，因此 $NS_3=S_4$. 所以 $S_4/N\cong S_3$. 该结论在第八章，四，3，1)中已给出.

2) 设 $N\lhd G$，$H<G$ 且 $(N\cup H)=N\cup H$. 则 $H/(N\cap H)\cong N\cup H/N$.

证 由该命题，$H/(N\cap H)\cong NH/N$. 由第八章，二，4，$NH<G$. 由第八章，二，4，注 4)，$NH=HN$. 由第八章，4，注 7)，$NH=(N\cup H)$. 由已知，$(N\cup H)=N\cup H$. 所以 $H/(N\cap H)\cong N\cup H/N$.

3) 若 $A<G$，$B<G$ 且 $A\lhd(A\cup B)$，则 $B/(A\cap B)\cong AB/A$.

证 因 $B<G$，$B\subset(A\cup B)$，故 $B<(A\cup B)$. 已知 $A\lhd(A\cup B)$，从而由该命题，$B/(A\cap B)\cong AB/A$.

4) 命题"设 $N\lhd G$，$H<G$，则 $N/(N\cap H)\cong NH/H$"不成立.

例 $N=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}\lhd S_4$，$H=S_3<S_4$. 由上面注 1)例知 $NS_3=S_4$. 从而有 $(1\ 2\ 3\ 4)\in NS_3$，$(1\ 2\ 3)\in S_3$，但 $(1\ 2\ 3\ 4)(1\ 2\ 3)(1\ 2\ 3\ 4)^{-1}=(1\ 2\ 4)\overline{\in} S_3$，于是 S_3 不是 NS_3 的不变子群，因此 NS_3/S_3 无意义.

49. 证 设 H 是 G 的一个 n 阶子群．往证 $H=N$. 如果证得 $H\subset N$,由 $|H|=|N|=n$,就有 $H=N$. 如果证得 $NH=N$,就有 $H\subset N$. 所以关键是证明 $NH=N$. 而证 $NH=N$ 可以转化为证明 $|NH/N|=1$. 因 $N\lhd G,H<G$,故由第八章,二,4,$NH<G$,即 $N\subset NH<G$. 由第八章,三,2,5),$N\lhd NH$,即 NH/N 是商群．由第八章,四,14,1),$NH/N<G/N$. 设 $|NH/N|=t$,已知 $|G/N|=m$,则由 Lagrange 定理,$t\,\Big|\,m$. 已知 $N\lhd G,H<G$,由上面 48 题,$H/(N\cap H)\cong NH/N$. 从而,$|H/(N\cap H)|=|NH/N|$,即 $\dfrac{|H|}{|N\cap H|}=t$,于是 $|H|=n=t\,\Big|\,N\cap H\,\Big|$,因此 $t\,\Big|\,n$. 所以 $t\,\Big|\,(m,n)=1$,又 t 是正整数,从而 $t=1$,即 $|NH/N|=1,NH=N,H\subset N$. 因 $|H|=|N|=n$,故 $H=N$. 命题得证.

50. 证一 1) 易证,$\forall a\in G,\psi:a\to\phi_a$ 是 G 到 $I(G)$ 的一个满射．$\forall a,b\in G,\psi:a\to\phi_a,b\to\phi_b,ab\to\phi_{ab}$,则 $\phi_{ab}=\phi_a\,\phi_b$. 事实上,$\forall x\in G,\phi_{ab}(x)=(ab)x(ab)^{-1}=a(bxb^{-1})a^{-1}=\phi_a(bxb^{-1})=\phi_a(\phi_b(x))=(\phi_a\,\phi_b)(x)$,于是 $\phi_{ab}=\phi_a\,\phi_b$. 所以 $G\overset{\psi}{\sim}I(G)$. 因 G 是群,故 $I(G)$ 也是群. 且 ϕ_e 是 $I(G)$ 的单位元．事实上,$\forall\,\phi_a\in I(G),\phi_a\phi_e=\phi_{ae}=\phi_a,\phi_e\,\phi_a=\phi_{ea}=\phi_a$,即 $\phi_a\,\phi_e=\phi_e\,\phi_a=\phi_a$. 所以 ϕ_e 是 $I(G)$ 的单位元.

2) 由 1),$G\overset{\psi}{\sim}I(G)$. 只需证明 $\ker\psi=Z$,由同态基本定理可知 $G/Z\cong I(G)$. 下面证明 $\ker\psi=Z$. $a\in\ker\psi\Leftrightarrow\psi(a)=\phi_a=\phi_e$,其中 ϕ_e 是 $I(G)$ 的单位元 $\Leftrightarrow\forall x\in G,\phi_a(x)=\phi_e(x)\Leftrightarrow\forall x\in G,axa^{-1}=exe^{-1}\Leftrightarrow\forall x\in G,ax=xa\Leftrightarrow a\in Z$. 因此 $\ker\psi=Z$. 所以 $G/Z\cong I(G)$.

3) 已知 Aut G 与 $I(G)$ 都对于变换乘法来说作成群,且 $I(G)\subset$ Aut G,从而 $I(G)<$ Aut G. $\forall\tau\in$ Aut $G,\phi_a\in I(G),\forall x\in G$,有 $(\tau\,\phi_a\tau^{-1})(x)=\tau\big(\phi_a(\tau^{-1}(x))\big)=\tau\big(a\tau^{-1}(x)a^{-1}\big)=\tau(a)\tau(\tau^{-1}(x))\tau(a^{-1})=\tau(a)\,x\,(\tau(a))^{-1}=\phi_{\tau(a)}(x)$,因此 $\tau\,\phi_a\tau^{-1}=\phi_{\tau(a)}\in I(G)$(因 $\tau(a)\in G$). 所以 $I(G)\lhd$ Aut G.

证二 1)、3)的证明见证一．2)还可如下证明.

$\sigma:aZ\to\phi_a$ 是 G/Z 与 $I(G)$ 间的一个同构映射．事实上,① $\forall aZ\in G/Z,\exists\,\phi_a\in I(G)$,使得 $\sigma(aZ)=\phi_a$. 若 $aZ=bZ$,则 $b^{-1}a\in Z$. 于是 $\forall x\in G,b^{-1}ax=xb^{-1}a$,从而 $(b^{-1}a)x(b^{-1}a)^{-1}=x$,即 $\phi_{b^{-1}a}(x)=x=\phi_e(x)$. 因此 $\phi_{b^{-1}}\,\phi_a=\phi_e$,即 $\phi_a=(\phi_{b^{-1}})^{-1}$. 因 $\phi_b\,\phi_{b^{-1}}=\phi_{bb^{-1}}=\phi_e$,故 $(\phi_{b^{-1}})^{-1}=\phi_b$,从而 $\phi_a=\phi_b$. 所以 σ 是 G/Z 到 $I(G)$ 的一个映射．② 显然 σ 是 G/Z 到 $I(G)$ 的一个满射．③ $\forall aZ,bZ\in G/Z$,若 $\phi_a=\phi_b$,则 $(\phi_b)^{-1}\phi_a=\phi_e$,即 $\phi_{b^{-1}}\phi_a=\phi_e$,从而 $\phi_{b^{-1}a}=\phi_e$. $\forall x\in G,\phi_{b^{-1}a}(x)=\phi_e(x)$,即 $(b^{-1}a)x(b^{-1}a)^{-1}=x$,有 $(b^{-1}a)x=x(b^{-1}a)$,于是 $b^{-1}a\in Z$,因此 $aZ=bZ$. 所以 σ 是单射．④ $\forall aZ,bZ\in G/Z,\sigma(aZ\cdot bZ)=\sigma(abZ)=\phi_{ab}=\phi_a\,\phi_b=\sigma(aZ)\sigma(bZ)$. 综上有 $G/Z\overset{\sigma}{\cong}I(G)$.

注 1) $\phi_a(\in I(G))$ 的逆元是 $\phi_{a^{-1}}$,且 $\phi_a\,\phi_b=\phi_{ab}$.

2) 由该命题容易证明下面命题:"非交换群 G 的内自同构群 $I(G)$ 不是循环群. 非交换群 G 的自同构群 Aut$G$ 也不是循环群.

证 设 Z 是 G 的中心．由第八章,四,12,G/Z 不是循环群. 由该命题 2),$G/Z\cong I(G)$,从而 $I(G)$ 不是循环群. 由该命题 3),$I(G)\lhd$ Aut$G$,从而 Aut$G$ 也不是循环群.

3) 设 G 不是交换群,且 G 的不变子群只有 $\{e\}$ 和本身. 则 $G\cong I(G)$.

证一 设 Z 是 G 的中心,则 $Z\lhd G$. 由已知条件,$Z=G$ 或 $Z=\{e\}$. 但 G 不是交换群,即

$G\neq Z$，因此只能 $Z=\{e\}$. 从而由该命题 2)，$G\cong G/\{e\}=G/Z\cong I(G)$，即 $G\cong I(G)$.

证二 由该命题 1)，$\forall a\in G,\psi:a\to\phi_a$ 是 G 到 $I(G)$ 的一个同态满射．下面证明在给定的条件下，ψ 是 G 到 $I(G)$ 的一个单射．$\forall a,b\in G$，若 $\phi_a=\phi_b$，则 $\forall x\in G,\phi_a(x)=\phi_b(x)$，即 $axa^{-1}=bxb^{-1}$，从而 $(b^{-1}a)x=x(b^{-1}a)$，于是 $b^{-1}a\in G$ 的中心 Z. 因 $Z\lhd G$，由 G 不是交换群，故 $Z\neq G$，再由已知条件，$Z=\{e\}$. 因此 $b^{-1}a=e$，即 $a=b$. 可见 ψ 是单射．所以 $G\cong I(G)$.

4） 若 G 是交换群，则 G 的内自同构只有恒等自同构 ϕ_e.

证 设 ϕ_a 是 G 的任一内自同构，$\forall x\in G,\phi_a(x)=axa^{-1}\xlongequal{\text{由 } G \text{ 是交换群}}xaa^{-1}=x=\phi_e(x)$. 从而 $\phi_a=\phi_e$.

例 设 4 阶循环群 $G=(\mathrm{i})=\{\mathrm{i}^0=1,\mathrm{i},\mathrm{i}^2=-1,\mathrm{i}^3=-\mathrm{i}\}$. 求出 Aut G 与 $I(G)$.

解 由第六章，二，6，注 3)，G 的生成元有且只有 i 与 i^3（因 $(3,4)=1$）. 由第六章，二，7，注 1)，G 的自同构必然把生成元映到生成元．我们知道，$\sigma_1:\mathrm{i}\to\mathrm{i}$，即 $\sigma_1:x\to x(\forall x\in G)$ 是 G 的一个自同构．$\sigma_2:\mathrm{i}\to\mathrm{i}^3$，即 $\sigma_2:1=\mathrm{i}^0\to(\mathrm{i}^0)^3=1,\mathrm{i}\to\mathrm{i}^3=-\mathrm{i},-1=\mathrm{i}^2\to(\mathrm{i}^2)^3=\mathrm{i}^6=\mathrm{i}^2=-1,-\mathrm{i}=\mathrm{i}^3\to(\mathrm{i}^3)^3=\mathrm{i}^9=\mathrm{i}$. 易证 σ_2 是 G 的一个自同构．因此，$\mathrm{Aut}G=\{\sigma_1,\sigma_2\}$. 因 G 是交换群，故 G 的内自同构只有恒等自同构 σ_1. 所以 $I(G)=\{\sigma_1\}$.

第九章

1. 解 1） R 不是环，因 R 无零元.

2） R 不是环，因有 $\sqrt{3}\in R$，但 $\sqrt{3}\cdot\sqrt{3}=3\overline{\in}R$.

3） R 不是环，因有 $\mathrm{i}\in R$，但 $\mathrm{i}\cdot\mathrm{i}=-1\overline{\in}R$.

4） R 不是环，因 R 无零元.

5） R 不是环．因 $(a+b\sqrt{2}+c\sqrt{5})(d+e\sqrt{2}+f\sqrt{5})=ad+(ae+bd)\sqrt{2}+(af+cd)\sqrt{5}+2be+5cf+(bf+ce)\sqrt{10}$，当 $bf+ce\neq0$ 时，$(a+b\sqrt{2}+c\sqrt{5})(d+e\sqrt{2}+f\sqrt{5})\overline{\in}R$.

6） R 是一个环．事实上，$\forall\frac{a}{b},\frac{c}{d}\in R,\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$，因 bd 是奇数，故 R 对于＋封闭．加法交换律与结合律成立．R 有零元 $\frac{0}{1}$. $\frac{a}{b}(\in R)$ 有负元 $\frac{-a}{b}\in R$. $\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$，因 bd 是奇数，故 R 对于·封闭．乘法结合律与乘法对加法的分配律显然成立．所以 R 是一个环.

7） R 是一个环．事实上，$\forall\frac{m_1}{2^{n_1}},\frac{m_2}{2^{n_2}}\in R,\frac{m_1}{2^{n_1}}+\frac{m_2}{2^{n_2}}=\frac{m_1 2^{n_2}+m_2 2^{n_1}}{2^{n_1+n_2}}\in R,\frac{m_1}{2^{n_1}}\cdot\frac{m_2}{2^{n_2}}=\frac{m_1m_2}{2^{n_1+n_2}}\in R$，从而 R 对＋与·封闭．加法交换律与结合律、乘法结合律与乘法对加法的分配律显然都成立．R 有零元 $\frac{0}{2^0}=0,\frac{m}{2^n}(\in R)$ 有负元 $\frac{-m}{2^n}\in R$. 所以 R 是一个环.

2. 解 1） R 不是环．取 $\begin{pmatrix}1&2\\2&4\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix}\in R,\begin{pmatrix}1&2\\2&4\end{pmatrix}\oplus\begin{pmatrix}0&1\\0&0\end{pmatrix}=\begin{pmatrix}1&3\\2&4\end{pmatrix}$，但 $\begin{vmatrix}1&3\\2&4\end{vmatrix}=-2\neq0$，从而 R 对于 $\oplus$ 不封闭.

2） R 不是环．因取 $1,-1,2\in R,(1\oplus(-1))\odot2=0\odot2=|0|2=0$，而 $(1\odot2)\oplus((-1)\odot2)=|1|2+|-1|2=2+2=4$，从而右分配律不成立.

3） R 不是环．因取 $1,3\in R,1\oplus3=1-3-2=-4$，而 $3\oplus1=3-1-2=0$，从而加法交换律不成立.

4) R 是一个环．事实上，因 R 对于＋与· 作成一个环，故 $a\oplus b=a+b-1\in R$，$a\odot b=a+b-ab\in R$ 且由 a,b 唯一确定，从而 R 对$\oplus$与$\odot$封闭．$\forall a,b,c\in R$，

$$\begin{aligned}a\oplus(b\oplus c)&=a\oplus(b+c-1)=a+(b+c-1)-1\\&=a+b+c-2\cdot 1.\\(a\oplus b)\oplus c&=(a+b-1)\oplus c=(a+b-1)+c-1\\&=a+b+c-2\cdot 1.\end{aligned}$$

于是 $a\oplus(b\oplus c)=(a\oplus b)\oplus c$. $\forall a,b\in R$，

$$a\oplus b=a+b-1=b+a-1=b\oplus a.$$

因此 $a\oplus b=b\oplus a$. 若 $\exists x\in R$，使得 $\forall a\in R$，$x\oplus a=a$，即 $x+a-1=a$，从而 $x=1$. 所以 $\exists 1\in R$，使得 $\forall a\in R$，$1\oplus a=1+a-1=a$，即 R 有零元 1. $\forall a\in R$，若 $\exists y\in R$，使得 $y\oplus a=1$，即 $y+a-1=1$，从而 $y=2\cdot 1-a$. 所以，$\forall a\in R$，$\exists 2\cdot 1-a\in R$，使得 $(2\cdot 1-a)\oplus a=2\cdot 1-a+a-1=1$，即 a 有负元 $2\cdot 1-a\in R$. 至此，已证明 R 作成加群．$\forall a,b,c\in R$，

$$\begin{aligned}(a\odot b)\odot c&=(a+b-ab)\odot c=(a+b-ab)+c-(a+b-ab)c\\&=a+b+c-ab-ac-bc+abc.\\a\odot(b\odot c)&=a\odot(b+c-bc)=a+(b+c-bc)-a(b+c-bc)\\&=a+b+c-bc-ab-ac+abc.\end{aligned}$$

于是 $(a\odot b)\odot c=a\odot(b\odot c)$. $\forall a,b,c\in R$，

$$\begin{aligned}a\odot(b\oplus c)&=a\odot(b+c-1)=a+(b+c-1)-a(b+c-1)\\&=2a+b+c-ab-ac-1.\\(a\odot b)\oplus(a\odot c)&=(a+b-ab)\oplus(a+c-ac)=(a+b-ab)+(a+c-ac)-1\\&=2a+b+c-ab-ac-1.\end{aligned}$$

于是 $a\odot(b\oplus c)=(a\odot b)\oplus(a\odot c)$. 同理可证 $(b\oplus c)\odot a=(b\odot a)\oplus(c\odot a)$. 所以 R 是一个环.

$\exists 0\in R$，使得 $\forall a\in R$，

$$0\odot a=0+a-0a=a,\quad a\odot 0=a+0-a0=a.$$

所以 R 有单位元 0.

3. 解 $\mathbb{Z}_5=\{[0],[1],[2],[3],[4]\}$.

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

·	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

4. 解 1) 设 $[4][a]=[3]$，则 $[4a-3]=[0]$，从而 $12\mid 4a-3$，即 $\exists q\in\mathbb{Z}$，使得 $4a-3=12q$，于是 $a=\dfrac{3+12q}{4}$. 因 $4\mid 12q$，但 $4\nmid 3$，故 $4\nmid 3+12q$. 即 $\bar{\exists} a\in\mathbb{Z}$，使得 $a=\dfrac{3+12}{4}q$. 所以方程 $[4]x=[3]$ 无解.

2） 设$[4][a]=[4]$，则$[4a-4]=[0]$，从而$12\mid 4(a-1)$，即$3\mid a-1$. 于是$\exists q\in\mathbb{Z}$，使得$a-1=3q$，即$a=3q+1$. q分别取0,1,2,3时，$a=1,4,7,10$. 所以方程$[4]x=[4]$有且只有4个解：$[1],[4],[7],[10]$.

3） 设$[a]^2-[1]=[0]$，则$[a^2-1]=[0]$，从而$12\mid a^2-1$. 于是$\exists q\in\mathbb{Z}$，使得$a^2-1=12q$，即$a^2=12q+1$. 当q分别取0,2时，$a=\pm1,\pm5$. 所以方程$x^2-1=0$有且只有4个解：$[1],[-1]=[11],[5],[-5]=[7]$.

5. 证 1） $(-b)a=-ba=-ab=a(-b)$.

2） $(nb)a=n(ba)=n(ab)=a(nb)$.

3） 因$ab=ba$，故$b^{-1}(ab)b^{-1}=b^{-1}(ba)b^{-1}$，即$b^{-1}a=ab^{-1}$.

4） 已知$ab=ba,ac=ca$，则

$$a(b+c)=ab+ac=ba+ca=(b+c)a.$$

5） 已知$ab=ba,ac=ca$，则

$$a(bc)=(ab)c=(ba)c=b(ac)=b(ca)=(bc)a.$$

6. 证 （$\Rightarrow$） 因a可逆，故$\exists a^{-1}\in R$，令$b=a^{-1}$. 由$ba=1$，有$aba=a$. 而且$baab=ab$，再由$ab=1$，有$ba^2b=1$.

（$\Leftarrow$）

$$ab=(ba^2b)(ab)=(ba)(aba)b=(ba)ab=ba^2b=1.$$

$$ba=(ba)(ba^2b)=b(aba)(ab)=ba(ab)=ba^2b=1.$$

从而$ab=ba=1$，所以$a^{-1}=b$，a可逆.

7. 证 设$(ab-1)^{-1}=x$，则$(ab-1)x=x(ab-1)=1$，即$abx-x=xab-x=1$. 由$abx-b^{-1}bx=1$，有$(a-b^{-1})bx=1$，由$bxabb^{-1}-bxb^{-1}=bb^{-1}$，有$bx(a-b^{-1})=1$. 从而$(a-b^{-1})^{-1}=bx$，$a-b^{-1}$可逆．[另一证法：设$(ab-1)^{-1}=x$，则$(b^{-1})^{-1}(ab-1)^{-1}=bx$，从而，$[(ab-1)b^{-1}]^{-1}=bx$，即$(a-b^{-1})^{-1}=bx$.]

$$\begin{aligned}&[(a-b^{-1})^{-1}-a^{-1}](aba-a)=(bx-a^{-1})(aba-a)\\&=bxaba-ba-bxa+1=b(1+x)a-ba-bxa+1\\&=ba+bxa-ba-bxa+1=1.\end{aligned}$$

$$\begin{aligned}&(aba-a)[(a-b^{-1})^{-1}-a^{-1}]=(aba-a)(bx-a^{-1})\\&=ababx-abx-ab+1=ab(1+x)-abx-ab+1\\&=ab+abx-abx-ab+1=1.\end{aligned}$$

所以$(a-b^{-1})^{-1}-a^{-1}$可逆，且

$$[(a-b^{-1})^{-1}-a^{-1}]^{-1}=aba-a.$$

8. 证一 因$(1-ab)^{-1}=x$，故$x(1-ab)=(1-ab)x=1$，即$x-xab=x-abx=1$，从而$xab=abx=x-1$. 因此

$$\begin{aligned}(1+bxa)(1-ba)&=1+bxa-ba-bxaba=1+bxa-ba-b(x-1)a\\&=1+bxa-ba-bxa+ba=1.\end{aligned}$$

$$\begin{aligned}(1-ba)(1+bxa)&=1-ba+bxa-babxa=1-ba+bxa-b(x-1)a\\&=1-ba+bxa-bxa+ba=1.\end{aligned}$$

所以$(1-ba)^{-1}=1+bxa$.

证二 因$(1-ab)^{-1}=x$,故$(1-ab)x=1$,即$x-abx=1$. 左乘b,右乘a,得$bxa-babxa=ba$,将ba移项,两边加1,得$1-ba+bxa-babxa=1$,即$(1-ba)(1+bxa)=1$.

又$x(1-ab)=1$,即$x-xab=1$. 从而左乘b,右乘a,得$bxa-bxaba=ba$,将ba移项,两边加1,得$1+bxa-ba-bxaba=1$,即$(1+bxa)(1-ba)=1$. 所以$(1-ba)^{-1}=1+bxa$.

9. 解 设$a+b\mathrm{i}$是R中的可逆元,又1是R的单位元,从而

$$(a+b\mathrm{i})^{-1}=\frac{1}{a+b\mathrm{i}}=\frac{a}{a^2+b^2}+\frac{-b}{a^2+b^2}\mathrm{i}\in R.$$

于是$\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\in\mathbb{Z}$. 因$a+b\mathrm{i}$是可逆元,故$a+b\mathrm{i}\neq 0$,即$a,b$不能同时为零. 若$a\neq 0$,则$b=0$,不然,如果$b$也$\neq 0$,那么$0<\left|\frac{a}{a^2+b^2}\right|<1$,即$\frac{a}{a^2+b^2}\overline{\in}\mathbb{Z}$. 因此$b=0$. 这时$\frac{a}{a^2+b^2}=\frac{a}{a^2}=\frac{1}{a}\in\mathbb{Z}$,所以$a=\pm1$. 于是$a+b\mathrm{i}=\pm1$. 若$a=0$,则$b\neq0$,这时$\frac{-b}{a^2+b^2}=\frac{-b}{b^2}=\frac{-1}{b}\in\mathbb{Z}$,所以$b=\pm1$,于是$a+b\mathrm{i}=\pm\mathrm{i}$. 以上说明了R中的可逆元只可能是$\pm1,\pm\mathrm{i}$.

另一方面,因$1\cdot1=1,(-1)(-1)=1,\mathrm{i}(-\mathrm{i})=(-\mathrm{i})\mathrm{i}=1$,故$\pm1,\pm\mathrm{i}$都是$R$的可逆元.

所以R有且只有4个可逆元:$\pm1,\pm\mathrm{i}$.

10. 证 由$ab=ac,ab-ac=0$,即$a(b-c)=0$,因$a\neq0$且a不是左零因子,故$b-c=0$,即$b=c$.

11. 证 若$ba\neq0$,已知$a(ba)=0$,又$a\neq0$,因此a是左零因子;若$ba=0$,已知$b\neq0$,$a\neq0$,因此a是右零因子.

12. 证 1) 设a是R的幂等元,则$a^2=a$,即$a^2-a=0$. 因R有单位元1,故$a(a-1)=0$. 因R无零因子,故$a=0$或$a=1$;反之,0与1显然是幂等元.

2) 设a是R的幂零元,则$\exists$正整数n,使得$a^n=0$. 于是集$P=\{m\mid a^m=0,\ m$是正整数$\}\neq\varnothing$,P有最小正整数m_0,使得$a^{m_0}=0$,而$a^{m_0-1}\neq0$. 因$a^{m_0}=aa^{m_0-1}=0$,又R无零因子,故$a=0$;反之,0显然是幂零元.(另一证法:若$a\in R,a\neq0$,对于任意正整数n,下面用数学归纳法证明:$a^n\neq0$. $n=2$时,因R无零因子,故$a^2=aa\neq0$. 假定k时,$a^k\neq0$,今看$k+1$时,因R无零因子,故$a^{k+1}=a^ka\neq0$. 由归纳原理,$\forall$正整数n,都有$a^n\neq0$,从而R中任意非零元都不是幂零元. 又零元0显然是幂零元,因此R有且只有零元0是幂零元.)

3) ($\Rightarrow$) 因e是R的非零幂等元,故$e^2=e$. $\forall a\in R,e^2a=ea$,即$e(ea)=ea$. 因$e\neq0$,又R无零因子,消去律成立,故$ea=a$. 同理,$ae=a$. 所以e是R的单位元.(另一证法:因$e^2=e$,故$\forall a\in R,e^2a=ea$,即$e(ea-a)=0$. 由R无零因子,$e\neq0$,有$ea-a=0$,即$ea=a$. 同理,$ae=a$. 所以e是单位元.)

($\Leftarrow$) 因e是R的单位元,故$e^2=ee=e$,又$R\neq\{0\}$,从而e是R的非零幂等元.

4) 设$a(\neq0)$是R的幂零元,则$\exists$正整数n,使得$a^n=0$. 于是集$P=\{m\mid a^m=0,m$是正整数$\}\neq\varnothing$,P中有最小正整数m_0,使得$a^{m_0}=0$,即$aa^{m_0-1}=a^{m_0-1}a=0$,其中$a^{m_0-1}\neq0$,$a\neq0$,所以a是R的零因子.

注　零因子未必是幂零元．如$\begin{pmatrix}1&0\\0&0\end{pmatrix}$是环$\left\{\begin{pmatrix}a&0\\0&b\end{pmatrix}\middle|a,b\in\mathbb{Z}\right\}$的零因子，但不是幂零元.

5）　因 x 是 R 的幂零元，故∃正整数 n，使得 $x^n=0$. 从而 $1-x^n=1-0=1$，于是

$$\begin{aligned}1-x^n&=(1-x)(1+x+x^2+\cdots+x^{n-1})\\&=(1+x+x^2+\cdots+x^{n-1})(1-x)=1.\end{aligned}$$

所以 $1-x$ 可逆且

$$(1-x)^{-1}=1+x+x^2+\cdots+x^{n-1}.$$

6）　因 $0\in S$，故 $S\neq\varnothing$ 且 $S\subset R$. $\forall a,b\in S$，a,b 都是 R 的幂零元，从而∃正整数 m,n，使得 $a^m=0,b^n=0$. 因 R 是交换环，故由第九章，二，3，有

$$(a+b)^{m+n}=a^{m+n}+\binom{m+n}{1}a^{m+n-1}b+\cdots+\binom{m+n}{n}a^mb^n+\binom{m+n}{n+1}a^{m-1}b^{n+1}+\cdots+b^{m+n}$$
$$=0,$$

从而 $a+b\in S$. 又

$$(-a)^m=\overbrace{(-a)(-a)\cdots(-a)}^{m个}=\begin{cases}a^m,m是偶数;\\-a^m,m是奇数\end{cases}=0,$$

从而 $-a\in S$. 所以 S 是 R 的子加群．因 R 是交换环，故 $(ab)^m=a^mb^m=0b^m=0$，从而 $ab\in S$. 显然在 S 中乘法适合结合律与分配律．综上可知，S 是一个环.

7）　①⇒②　若 $a\in R$ 且 $a^2=0$，则必 $a=0$. 不然，若 $a\neq0$，但 $a^2=0$，从而 R 有非零的幂零元 a，此与已知矛盾．所以 $a=0$.

②⇒①　若 a 是 R 的幂零元，则必 $a=0$. 不然，若 $a\neq0$，由已知 $a^2\neq0$，再由已知 $(a^2)^2=a^4\neq0$，如此继续下去，∀正整数 n，使得 $a^{2^n}\neq0$. 因 a 是幂零元，故∃正整数 m，使得 $a^m=0$. 我们总可取到正整数 n_1，使得 $2^{n_1}>m$，令 $2^{n_1}=m+t$，其中 t 是正整数，于是 $a^{2^{n_1}}=a^{m+t}=a^ma^t=0$，此与∀正整数 n，使得 $a^{2^n}\neq0$ 矛盾．所以 $a=0$，即 R 无非零的幂零元.

注　1）　本题 1）中去掉 R 无零因子条件后，在一般有单位元 1 的环 R 中，R 的幂等元未必只有 0 与 1. 例，在 $\mathbb{Z}_6$ 中，幂等元除 0=[0]与 1=[1]外，还有[3]，[4]，因为$[3]^2=[3]$，$[4]^2=[4]$.

2）　本题 2）的逆命题不成立．即环 R 的幂零元有且只有 0 时，R 可能有零因子．例，$\mathbb{Z}_6$ 有且只有 0=[0]是幂零元，但 $\mathbb{Z}_6$ 有零因子[2]，[3]，[4].

3）　本题 3）中条件可改为：若环 R 中有非零幂等元 e，且 e 不是左零因子，也不是右零因子，则 e 是 R 的单位元．由 3）可知，在无零因子环 $R(\neq\{0\})$ 中，因左（右）单位元都是非零幂等元，故左（右）单位元都是单位元．当 $R=\{0\}$ 时，显然 R 的左（右）单位元是单位元（见第九章，三，1，6））.

4）　本题 4）的逆命题不成立．例，在 $\mathbb{Z}_6$ 中，[2]是零因子，但[2]不是幂零元.

5）　由本题 6）的证明知，在交换环中，若 a 与 b 是幂零的，则 $a+b$ 也是幂零的．对于非交换环，这个命题不对．例，$R=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\middle|a,b,c,d\in\mathbb{Z}\right\}$为非交换环．因$\begin{pmatrix}0&1\\0&0\end{pmatrix}^2=\begin{pmatrix}0&0\\0&0\end{pmatrix}$，$\begin{pmatrix}0&0\\1&0\end{pmatrix}^2=\begin{pmatrix}0&0\\0&0\end{pmatrix}$，故$\begin{pmatrix}0&1\\0&0\end{pmatrix}$，$\begin{pmatrix}0&0\\1&0\end{pmatrix}$是 R 的幂零元．但$\begin{pmatrix}0&1\\0&0\end{pmatrix}+\begin{pmatrix}0&0\\1&0\end{pmatrix}=$

$\begin{pmatrix}0&1\\1&0\end{pmatrix}$. 由 $\forall$ 正整数 n, $\begin{pmatrix}0&1\\1&0\end{pmatrix}^n=\begin{cases}\begin{pmatrix}1&0\\0&1\end{pmatrix}, n\text{ 是偶数时};\\ \begin{pmatrix}0&1\\1&0\end{pmatrix}, n\text{ 是奇数时}\end{cases}\neq\begin{pmatrix}0&0\\0&0\end{pmatrix}$, 所以 $\begin{pmatrix}0&1\\1&0\end{pmatrix}$ 不是幂零元. 此例也可说明:若环 R 不是交换环,本题中命题 6)不成立.

13. 证 1) $\forall x\in R$,

$$\begin{aligned}x+x&=(x+x)^2=(x+x)(x+x)=x^2+x^2+x^2+x^2\\&=x+x+x+x.\end{aligned}$$

因 R 是环,故 $-x\in R$,且

$$x+x+(-x)+(-x)=x+x+x+x+(-x)+(-x).$$

即 $x+x=0$.(另一证法:$\forall x\in R$, $-x\in R$,从而 $x=x^2=(-x)^2=-x$,所以 $x+x=0$.)

2) $\forall x,y\in R$,

$$x+y=(x+y)^2=x^2+yx+xy+y^2=x+yx+xy+y,$$

从而 $yx+xy=0$. 两边加 yx,得 $yx+yx+xy=yx$. 由 1)知 $yx+yx=0$,从而 $xy=yx$.

注 1) 在布尔环 R 中,任意元的负元是自身,即,$\forall x\in R$, $-x=x$.

2) 布尔环是交换环.

例 1 $R=\{0,1\}$对于

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

作成一个布尔环.

例 2 给定一个集 I,将 I 的全部子集作成的集记为 S,即 $S=\{A\mid A\subset I\}$. $\forall A,B\in S$,规定

$$A+B=(A-B)\cup(B-A),\ AB=A\cap B.$$

则 S 作成一个布尔环.

14. 证一 只需证明在 R 中加法交换律成立.

若 $R=\{0\}$,命题显然成立.

若 $R\neq\{0\}$,则 $\exists c\in R$, $c\neq 0$. $\forall a,b\in R$,有

$$\begin{aligned}(c+c)(a+b)&\xlongequal{\text{左分配律}}(c+c)a+(c+c)b\\&\xlongequal{\text{右分配律}}(ca+ca)+(cb+cb)\xlongequal{\text{结合律}}ca+ca+cb+cb.\end{aligned}$$

$$\begin{aligned}(c+c)(a+b)&\xlongequal{\text{右分配律}}c(a+b)+c(a+b)\\&\xlongequal{\text{左分配律}}(ca+cb)+(ca+cb)\xlongequal{\text{结合律}}ca+cb+ca+cb.\end{aligned}$$

从而

$$ca+ca+cb+cb=ca+cb+ca+cb.$$

由 $-ca$, $-cb\in R$ 且 R 对加法封闭,有

$$(-ca)+ca+ca+cb+cb+(-cb)=(-ca)+ca+cb+ca+cb+(-cb).$$

由加法适合结合律及负元、零元定义,有 $ca+cb=cb+ca$,由左分配律,$c(a+b)=c(b+a)$,由

负元定义，$c(a+b)+[-c(b+a)]=0$，即 $c(c+b)+c[-(b+a)]=0$，再由左分配律，$c\{(a+b)+[-(b+a)]\}=0$. 因 $c\neq0$，R 无零因子，故$(a+b)+[-(b+a)]=0$. 从而 $a+b=b+a$. 所以 R 是一个环.

证二 若 $R=\{0\}$，命题显然成立.

若 $R\neq\{0\}$，则 $\exists\, c\in R$，$c\neq0$. $\forall\, a,b\in R$，有

$$\begin{aligned}c[(a+b)-(b+a)]&=c\{(a+b)+[-(b+a)]\}\\&=c(a+b)+c[-(b+a)]=c(a+b)+[-c(b+a)]\\&=c(a+b)+(-c)(b+a)=ca+cb+(-c)b+(-c)a\\&=ca+cb+(-cb)+(-ca)=ca+0+(-ca)=0.\end{aligned}$$

因 R 无零因子，$c\neq0$，故$(a+b)-(b+a)=0$，从而 $a+b=b+a$. 所以 R 是一个环.

注 与第九章，二，5，注同样，下面的证法是错误的：$\forall\, a,b\in R$，

$$a+b-(b+a)=a+b-b-a=0,$$

从而 $a+b=b+a$.

第十章

1. 解 1) 易证 F 是一个含非零元的交换环，有单位元$\begin{pmatrix}1&0\\0&1\end{pmatrix}$. $\forall\begin{pmatrix}a&b\\2b&a\end{pmatrix}\in F$，$\begin{pmatrix}a&b\\2b&a\end{pmatrix}\neq\begin{pmatrix}0&0\\0&0\end{pmatrix}$，即 a,b 不同时为零. 于是$\begin{vmatrix}a&b\\2b&a\end{vmatrix}=a^2-2b^2\neq0$，事实上，若$\begin{vmatrix}a&b\\2b&a\end{vmatrix}=a^2-2b^2=0$，则 $a^2=2b^2$. 因 a,b 不同时为零，故 $a\neq0,b\neq0$，从而$\frac{a^2}{b^2}=2$，即$\frac{a}{b}=\pm\sqrt{2}$，左边是有理数，但右边是无理数，矛盾. 因此$\begin{pmatrix}a&b\\2b&a\end{pmatrix}$是可逆矩阵. 所以 $\exists\begin{pmatrix}a&b\\2b&a\end{pmatrix}^{-1}=\frac{1}{a^2-2b^2}\begin{pmatrix}a&-b\\-2b&a\end{pmatrix}\in F$，使得$\begin{pmatrix}a&b\\2b&a\end{pmatrix}^{-1}\begin{pmatrix}a&b\\2b&a\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$. 即 F 的每一个非零元都有逆元. 综上可知 F 是域.

2) F 不是域. 因为 $A=\left(\begin{pmatrix}\sqrt{2}&1\\2&\sqrt{2}\end{pmatrix}\left(\neq\begin{pmatrix}0&0\\0&0\end{pmatrix}\right)\right)\in F$，但$|A|=0$，$A$ 不可逆，即 A 在 F 中无逆元.

3) F 是域. 记 $F=\mathbb{Q}(\sqrt[3]{5})$.

4) F 是域. 称 F 为复数域 $\mathbb{C}$ 上的有理函数域.

2. 证 (反证法)假设ϕ是加群 R 与乘群 R^* 间的一个同构映射，则$\phi(0)=1$，其中 0 是加群 R 的零元，1 是乘群 R^* 的单位元. 取 $-1\in R^*$，因ϕ是满射，故 $\exists\, a\in R$，使得$\phi(a)=-1$. 下面证明 $1=-1$：

1) 当 $a=0$ 时，由ϕ是映射知 $1=-1$.

2) 当 $a\neq0$ 时，$\phi(a+a)=\phi(a)\phi(a)=(-1)(-1)=1$. 又已知$\phi(0)=1$，由$\phi$是单射，$a+a=0$，从而，$a(1+1)=a1+a1=a+a=0$. 因 $a\neq0$，除环 R 无零因子，故 $1+1=0$，即$1=-1$.

因而，在任何情况下都有 $1=-1$. 由此有

$$\phi(1)\phi(1)=\phi(1+1)=\phi(1+(-1))=\phi(0)=1.$$

即 $\phi(1)\phi(1)-1=0$. 从而

$$\begin{aligned}(\phi(1)-1)(\phi(1)-1)&=(\phi(1)-1)(\phi(1)+(-1))=(\phi(1)-1)(\phi(1)+1)\\&=\phi(1)\phi(1)-\phi(1)+\phi(1)-1=\phi(1)\phi(1)-1=0.\end{aligned}$$

因除环 R 无零因子，故 $\phi(1)-1=0$，即 $\phi(1)=1$. 已知 $\phi(0)=1$，因 ϕ 是单射，故 $1=0$，此与除环 $R\neq\{0\}$ 矛盾. 所以加群 R 与乘群间不存在同构映射.

3. 证 $\forall a\in R$.

1) $a\neq0$ 时，因 R 是除环，故 $R^*=R-\{0\}$ 是 $q-1$ 阶乘群. 今 $a\in R^*$，由第七章，三，1，7)，$a^{q-1}=1$，即 $a^qa^{-1}=1$，所以 $a^q=a$.

2) $a=0$ 时，显然有 $a^q=a$. 综上，$\forall a\in R$，有 $a^q=a$.

4. 证 1 没有右拟逆元. 事实上，$\forall x\in R$，$1+x-1x=1\neq0$，从而除环 R 中任意元都不是 1 的右拟逆元.

$\forall a\in R$，$a\neq1$，a 必有右拟逆元. 事实上，若 $a+b-ab=0$，即 $(1-a)b=-a$. 因 $1-a\neq0$，而 R 是除环，故 $1-a$ 有逆元 $(1-a)^{-1}\in R$，使得 $(1-a)^{-1}(1-a)b=-(1-a)^{-1}a$，即 $b=-(1-a)^{-1}a$. 且

$$\begin{aligned}&a+\{-(1-a)^{-1}a\}-a\{-(1-a)^{-1}a\}\\=&a-(1-a)^{-1}a+a(1-a)^{-1}a\\=&a-(1-a)(1-a)^{-1}a\\=&a-a=0.\end{aligned}$$

所以 $-(1-a)^{-1}a$ 是 a 的右拟逆元.

5. 证一 （反证法）若有只含 6 个元的整环 R. 由第四章，二，6 知，R 的特征是素数 p①，且 $p\mid 6$，从而 $p=2$ 或 3.

当 $p=2$ 时，取 $a,b\in R$，$a\neq0$，$b\neq0$. 因 a 与 b 的阶都 $=2$，故集 $\{a,b\}$ 生成的加群 R 的子加群 $(\{a,b\})=\{0,a,b,a+b\}$，它的阶是 4，从而由 Lagrange 定理，$4\mid 6$，此为不可能.

当 $p=3$ 时，由第四章二，5，在一个有限群里阶大于 2 的元的个数一定是偶数，今有限加群 R 的阶为 3 的元的个数是 5，因而矛盾.

所以没有只含 6 个元的整环.

证二 （反证法）若有只含 6 个元的整环 R. 由证一，$\mathrm{ch}\,R=$ 素数 p 且 $p=2$ 或 3.

当 $p=2$ 时，取 $a_1\in R$，$a_1\neq0$. 因 R 是加群，故 a_1 生成的循环子群 (a_1) 是 R 的 2 阶不变子群. 从而商群 $R/(a_1)$ 的阶为 $\frac{|R|}{|(a_1)|}=\frac{6}{2}=3$. 设 $R/(a_1)=\{(a_1),a_2+(a_1),a_3+(a_1)\}$，其中 $a_2,a_3\in R$，$a_2\overline{\in}(a_1)$，$a_3\overline{\in}(a_1)$，(a_1) 是加群 $R/(a_1)$ 的零元. 因 $a_2+(a_1)$ 在 $R/(a_1)$ 中的阶为 3，故 $3(a_2+(a_1))=(a_1)$；另一方面，因 a_1 在 R 中的阶为 2，故 $3(a_2+(a_1))=3a_2+(a_1)=2a_2+a_2+(a_1)=a_2+(a_1)$，于是，$(a_1)=a_2+(a_1)$，产生矛盾.

当 $p=3$ 时，取 $a_1\in R$，$a_1\neq0$，则 a_1 的阶 $|a_1|=3$. 从而 a_1 生成的循环子群 $(a_1)=\{0,a_1,$

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 95. 定理 1；96. 定义和定理 2.

$2a_1\}$是加群R的3阶不变子群,其中,因$3a_1=0$,故$-a_1=2a_1$.于是商群$R/(a_1)$的阶为2.设$R/(a_1)=\{(a_1),a_2+(a_1)\}$,其中$a_2\in R$,$a_2\overline{\in}(a_1)$,$(a_1)$是加群$R/(a_1)$的零元.因$a_2+(a_1)$在$R/(a_1)$中的阶为2,故$2(a_2+(a_1))=(a_1)$;另一方面,$2(a_2+(a_1))=2a_2+(a_1)$,于是,$(a_1)=2a_2+(a_1)$.但$2a_2\overline{\in}(a_1)$.事实上,因$a_2$在$R$中的阶$=3$,故$2a_2\neq 0$.若$2a_2=a_1$,则$2a_2+a_2=a_1+a_2$,因$|a_2|=3$,故$0=a_1+a_2$,从而$a_2=-a_1=2a_1\in(a_1)$,矛盾.因此$2a_2\neq a_1$.若$2a_2=2a_1$,则$a_1+2a_2+a_2=a_1+2a_1+a_2$,即$a_1+3a_2=3a_1+a_2$,因$|a_2|=|a_1|=3$,故$a_1=a_2$,矛盾.因此$2a_2\neq 2a_1$.于是$2a_2\overline{\in}(a_1)$,这样就与$(a_1)=2a_2+(a_1)$发生矛盾.

所以不存在只含6个元的整环.

证三 (反证法)若有只含6个元的整环R.由证一,ch $R=2$或3且知ch $R=3$是不可能的,从而ch $R=2$.

因R是$\neq\{0\}$的无零因子的有限环,故由第十章,二,3,R是除环,从而$R^*=R-\{0\}$是5阶循环乘群,可设$R^*=(a)=\{1,a,a^2,a^3,a^4\}$,于是$R=\{0,1,a,a^2,a^3,a^4\}$.下面证明$1+a\overline{\in}R$.事实上:

1) 若$1+a=0$,则由ch $R=2$,$a=-1=1$,矛盾.

2) 若$1+a=1$,由加法消去律,$a=0$,矛盾.

3) 若$1+a=a$,由加法消去律,$1=0$,矛盾.

4) 若$1+a=a^2$,由ch $R=2$,有

$$a^3-1=(a-1)(1+a+a^2)=(a-1)(2a^2)=0,$$

从而$a^3=1$,矛盾.

5) 若$1+a=a^3$,则

$$\begin{aligned}a^3-1&=(a-1)(a^2+a+1)=(a-1)(a^2+a^3)=a^3+a^4-a^2-a^3\\&=a^4-a^2=a^2(a^2-1)=a^2(a+1)(a-1)=a^2a^3(a-1)=a^5(a-1).\end{aligned}$$

因R^*是5阶乘群,故$a^5=1$,从而$a^3-1=a-1$.由加法消去律,$a^3=a$,矛盾.

6) 若$1+a=a^4$,则

$$a^2-1=(a-1)(a+1)=(a-1)a^4=a^5-a^4=1-a^4.$$

从而$a^4+a^2-2\cdot 1=0$.因ch $R=2$,故$2\cdot 1=0$,于是$a^4+a^2=0$,即$a^4=-a^2$,由ch $R=2$,$a^4=a^2$,矛盾.

综上,$1+a\overline{\in}R$.此与R对+封闭矛盾.所以没有只含6个元的整环.

注 由证明可见,也不存在只含6个元的无零因子环.

6. 证一 1) 因F是一个有限域,故由第四章,二,6,F的特征是有限整数.可设ch F=素数p,则F的非零元对于加法来说的阶是p.因加群F的阶为5,故$p\mid 5$,从而p只能是1或5,但p是素数,所以ch $F=p=5$.

2) (反证法)若F^*不是4阶循环群,由第七章,二,11,F^*与Klein四元群同构,从而F^*中除单位元1以外每个元的阶都是2,所以$(1+1)^2=1$.但由分配律,有

$$(1+1)^2=1^2+1^2+1^2+1^2=1+1+1+1=4\cdot 1.$$

于是$4\cdot 1=1$,由加法适合消去律,$3\cdot 1=0$,此与ch $F=5$矛盾.因此F^*是一个4阶循环群.

证二 1) 见证一.

2) 因ch $F=5$,故F的单位元$1(\neq 0)$对于加法来说的阶是5,从而$0\cdot 1,1\cdot 1,2\cdot 1,3\cdot 1,4\cdot 1$互不相同(见第四章,一,7).又$F$含5个元,于是$F=\{0\cdot 1,1\cdot 1,2\cdot 1,3\cdot 1,$

$4\cdot 1\}$，其乘群 $F^*=\{1,2\cdot 1,3\cdot 1,4\cdot 1\}$. 因 $2\cdot 1\neq 1,(2\cdot 1)^2=4\cdot 1\neq 1,(2\cdot 1)^3=8\cdot 1=3\cdot 1\neq 1,(2\cdot 1)^4=16\cdot 1=15\cdot 1+1=0+1=1$，故 $2\cdot 1$ 对乘法来说阶是 4，即 4 阶群 F^* 中有 4 阶元 $2\cdot 1$，所以 F^* 是 4 阶循环群.

证三 1) 见证一.

2) $\exists x\in F^*$，而 $x\neq 1$ 且 $x\neq -1$. 于是 x 的阶 $|x|=4$. 事实上，$|x|\,\big|\,|F^*|=4$，因此 $|x|$ 是 1 或 2 或 4. 因 $x\neq 1$，故 $|x|\neq 1$. 若 $|x|=2$，则 $x^2=1$，从而 $x^2-x=1-x$，即 $-x(1-x)=1-x$，而 $1-x\neq 0$，由域 F 乘法适合消去律，有 $-x=1$，即 $x=-1$，此与 x 的取法矛盾，于是 $|x|\neq 2$. 所以 $|x|=4$. 因 4 阶群 F^* 含有 4 阶元 x，故 F^* 是 4 阶循环群.

第十一章

1. 解 1) 不正确. 因 A 可能不是 R 的子环. 但当 S_i 是 R 的含 A 的所有子环时，$\bigcup S_i\supset R$. 又 $\bigcup S_i\subset R$，从而 $\bigcup S_i=R\in N$.

2) 不正确. 例，$\mathbb{C}$ 是复数域，整数环 $\mathbb{Z}$ 是 $\mathbb{C}$ 的子环，但 $\mathbb{Z}$ 不是域.

3) 不正确. 当 $n\neq\pm 1$ 时，$n\mathbb{Z}$ 无单位元.

4) 正确. 事实上，ϕ：$[0]\to[0],[1]\to[1],[2]\to[2],[3]\to[3],[4]\to[0],[5]\to[1],[6]\to[2],[7]\to[3]$ 是 $\mathbb{Z}_8$ 到 $\mathbb{Z}_4$ 的一个同态满射.

5) 不正确. 因为 $(1,2)(\in\mathbb{Z}\times\mathbb{Z})$ 在 ϕ 下无逆象. 但 ϕ 是 $\mathbb{Z}$ 到 $\mathbb{Z}\times\mathbb{Z}$ 的单射的同态映射.

6) 正确. 因为域 $F=\{0,1\}$ 的代数运算必为：

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

7) 正确. 因为恰含三个元的整环 $R=\{0,1,a\}$ 的代数运算必为：

+	0	1	a
0	0	1	a
1	1	a	0
a	a	0	1

·	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

8) 正确. 由定义易证.

9) 正确. 事实上，$\forall\alpha\in R$，$\exists$ 不全为零的元 $\alpha,-1\in R$，使得 $\alpha+(-1)\alpha=0$. 从而 R 中任意元 α 不是 R 上未定元.

10) 正确. 由定义可证明. 这里要注意，当 R 不是整环时，$f(x)\neq 0,g(x)\neq 0$，未必有

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x).$$

例，在 $\mathbb{Z}_4[x]$ 中，

$$([2]x^2+[3]x+[2])([2]x^3+[3]) = [2]x^4+[2]x^2+[3]x+[2]$$

乘积的次数 $4\neq 2+3$.

11) 正确. 事实上，($\Rightarrow$) 因 $f(x)$ 是 $R[x]$ 的可逆元，故 $\exists g(x)\in R[x]$，使得 $f(x)g(x)=1$，于是 $\deg(f(x)g(x))=\deg 1$，由本题 10) 知，$\deg f(x)+\deg g(x)=0$. 又

$\deg f(x)\geqslant 0$，$\deg g(x)\geqslant 0$，从而 $\deg f(x)=0$ 且 $\deg g(x)=0$. 所以 $f(x)\in R$ 且 $g(x)\in R$. 因此 $f(x)$是 R 的可逆元.

($\Leftarrow$) 因 $f(x)(\in R\subset R[x])$是 R 的可逆元，故 $\exists\, g(x)\in R\subset R[x]$，使得 $f(x)g(x)=g(x)f(x)=1$，从而 $f(x)$是 $R(x)$的可逆元.

若 R 是整数环 $\mathbb{Z}$，则 $\mathbb{Z}[x]$的可逆元有且只有 ± 1. 若 R 是域，则 $R[x]$的可逆元有且只有 R 中的所有的非零元.

这里还要注意，当 R 不是整环时，命题不成立．例，在 $\mathbb{Z}_4[x]$中，

$$([2]x^2+[1])([2]x^2+[1])=[1],$$

从而$[2]x^2+[1]$是 $\mathbb{Z}_4[x]$的可逆元，但$[2]x^2+[1]\overline{\in}\mathbb{Z}_4$.

2. 证 1) 因 $p\nmid 1$，故$\frac{1}{1}=1\in S$，从而$\varnothing\neq S\subset R$. $\forall\frac{a_1}{b_1},\frac{a_2}{b_2}\in S$，其中 $a_1,b_1,a_2,b_2\in\mathbb{Z}$，$p\nmid b_1,p\nmid b_2$，有

$$\frac{a_1}{b_1}-\frac{a_2}{b_2}=\frac{a_1b_2-a_2b_1}{b_1b_2},\quad \frac{a_1}{b_1}\frac{a_2}{b_2}=\frac{a_1a_2}{b_1b_2}.$$

因上面两式右边的分子与分母都是整数，且 $p\nmid b_1b_2$，故$\frac{a_1}{b_1}-\frac{a_2}{b_2},\frac{a_1}{b_1}\frac{a_2}{b_2}\in S$，从而 S 是 R 的子环.

2) 证略.

3) 因 $0m=0\in S$，故$\varnothing\neq S\subset R$. $\forall\, x_1m,x_2m\in S$，由于在有理数环中分配律、交换律成立，有

$$x_1m-x_2m=(x_1-x_2)m\in S,\quad (x_1m)(x_2m)=(x_1x_2m)m\in S.$$

所以 S 是 R 的一个子环.

4)—12)证略.

3. 证 1) 显然$\mathbb{Q}(\omega)\subset\mathbb{C}$，$\omega(\neq 0)\in\mathbb{Q}(\omega)$. $\forall\, a+b\omega,c+d\omega\in\mathbb{Q}(\omega)$，有

$$(a+b\omega)-(c+d\omega)=(a-c)+(b-d)\omega\in\mathbb{Q}(\omega).$$

因 $\omega^2=-\omega-1$，故

$$(a+b\omega)(c+d\omega)=ac+(bc+ad)\omega+bd\omega^2$$

$$=ac+(bc+ad)\omega+bd(-\omega-1)=(ac-bd)+(bc+ad-bd)\omega\in\mathbb{Q}(\omega).$$

$\forall\, a+b\omega\in\mathbb{Q}(\omega)$，$a+b\omega\neq 0$，

$$\frac{1}{a+b\omega}=\frac{a-b-b\omega}{(a+b\omega)(a-b-b\omega)}=\frac{a-b-b\omega}{a^2-ab+b^2},$$

其中 $a^2-ab+b^2\neq 0$. 不然，若 $a^2-ab+b^2=0$，又

$$a^2-ab+b^2=\frac{a^2+b^2}{2}+\frac{(a-b)^2}{2},$$

从而 $\frac{a^2+b^2}{2}+\frac{(a-b)^2}{2}=0$，即 $a^2+b^2+(a-b)^2=0$，因此 $a=b=0$，与 $a+b\omega\neq 0$ 矛盾. 于是 $\exists\,\alpha=\frac{a-b-b\omega}{a^2-ab+b^2}\in\mathbb{Q}(\omega)$，使得

$$(a+b\omega)\alpha=\alpha(a+b\omega)=1.$$

所以 $a+b\omega$ 有逆元$\frac{a-b-b\omega}{a^2-ab+b^2}\in\mathbb{Q}(\omega)$.

综上，$\mathbb{Q}(\omega)$是 $\mathbb{C}$ 的子域.

2) 显然，$S\subset F$. 域 F 有单位元 1. 设 $\sigma(1)=x$. 因 σ 不是 F 的零同态，故 $\exists\, a\in F$，使得

$\sigma(a)\neq 0$，又 $\sigma(a)=\sigma(a1)=\sigma(a)\sigma(1)=\sigma(a)x$. 因域 F 中消去律成立，故 $x=1$，从而$\sigma(1)=1$，即 $1(=0)\in S$. $\forall a,b\in S$，

$$\sigma(a-b)=\sigma(a)-\sigma(b)=a-b,$$

从而 $a-b\in S$. $\forall a,b\in S,b\neq 0,\sigma(b)\sigma(b^{-1})=\sigma(bb^{-1})=\sigma(1)=1$，因此 $\sigma(b^{-1})=[a(b)]^{-1}$，于是

$$\sigma(ab^{-1})=\sigma(a)\sigma(b^{-1})=\sigma(a)[\sigma(b)]^{-1}=ab^{-1},$$

从而 $ab^{-1}\in S$. 所以 S 是 F 的子域.

4. 证 1) 因 $0a=0\in S$，故$\varnothing\neq S\subset R$. $\forall r_1a,r_2a\in S$，

$$r_1a-r_2a=(r_1-r_2)a\in S,\quad (r_1a)(r_2a)=(r_1ar_2)a\in S.$$

所以 S 是 R 的子环.

2)—3) 略.

5. 证 因为 $0\in S_i$，$i=1,2$，所以 $0\in S_1\cap S_2\neq\varnothing$ 显然 $S_1\cap S_2\subset R$. $\forall a,b\in S_1\cap S_2$，有 $a,b\in S_1$，$a,b\in S_2$，因 S_1,S_2 是 R 的子环，故 $a-b,ab\in S_i$，$i=1,2$，从而 $a-b,ab\in S_1\cap S_2$. 于是 $S_1\cap S_2$ 是 R 的子环.

其余情况请读者自证.

注 1) 环(整环、除环、域)的任意多个子环(整环、除环、域)的交仍是 R 的子环(整环、除环、域).

2) 整数环 $\mathbb{Z}$ 的两个子环 $3\mathbb{Z}$ 与 $5\mathbb{Z}$ 的交 $3\mathbb{Z}\cap 5\mathbb{Z}=15\mathbb{Z}$ 是 $\mathbb{Z}$ 的子环. 事实上，$\forall 15n\in 15\mathbb{Z}$，有 $15n=3\times 5n=5\times 3n$，从而 $15n\in 3\mathbb{Z}\cap 5\mathbb{Z}$，即 $15\mathbb{Z}\subset 3\mathbb{Z}\cap 5\mathbb{Z}$. 反之，$\forall m\in 3\mathbb{Z}\cap 5\mathbb{Z}$，有 $m=3q_1=5q_2$，$q_1,q_2\in\mathbb{Z}$，即 $3\mid m$，$5\mid m$. 因 $(3,5)=1$，故 $3\times 5=15\mid m$，即 $m=15q\in 15\mathbb{Z}$，从而 $3\mathbb{Z}\cap 5\mathbb{Z}\subset 15\mathbb{Z}$. 所以 $3\mathbb{Z}\cap 5\mathbb{Z}=15\mathbb{Z}$.

6. 解 $\mathbb{Z}_8$ 的子环是加群 $\mathbb{Z}_8$ 的子加群. 且 $\mathbb{Z}_8$ 是循环加群[①]. 由第七章，二，3，$\mathbb{Z}_8$ 的子加群是循环加群，从而 $\mathbb{Z}_8$ 的全部子加群是以下 4 个：

$$S_1=([0])=\{[0]\},S_2=([1])=\mathbb{Z}_8=([3])=([5])=([7]),$$

$$S_3=([2])=\{[0][2][4][6]\}=([6]),S_4=([4])=\{[0],[4]\}.$$

易验证子加群 S_1,S_2,S_3,S_4 即为 $\mathbb{Z}_8$ 的所有子环.

7. 证 设矩阵 $E_{ij}=\begin{pmatrix} & \overset{j\text{列}}{\vdots} & & \\ \cdots & 1 & \cdots & \cdots \\ & \vdots & & \\ & \vdots & & \end{pmatrix} i\text{行}\in M_n(R)$，其中 i 行 j 列交叉处的元是 1，其他元都是 0. 则 $\forall (a_{ij})\in M_n(R)$ 的中心 Z，有

$$(a_{ij})E_{ij}=E_{ij}(a_{ij}).$$

即

$$i\text{行}\begin{pmatrix} \cdots & \overset{j\text{列}}{a_{1i}} & \cdots \\ \cdots & a_{2i} & \cdots \\ & \vdots & \\ \cdots & a_{ii} & \cdots \\ \cdots & a_{ni} & \cdots \end{pmatrix}=\begin{pmatrix} \vdots & \vdots & & \overset{j\text{列}}{\vdots} & & \vdots \\ a_{j1} & a_{j2} & \cdots & a_{jj} & \cdots & a_{jn} \\ \vdots & \vdots & & \vdots & & \vdots \end{pmatrix} i\text{行}.$$

---

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 57. 例 2.

于是

$$a_{1i}=a_{2i}=\cdots=a_{i-1,i}=a_{i+1,i}=\cdots=a_{ni}=0,$$
$$a_{j1}=a_{j2}=\cdots=a_{j,j-1}=a_{j,j+1}=\cdots=a_{jn}=0,$$

令

$$a_{ii}=a_{jj}=a,$$

$i,j=1,2,\cdots,n$. 因此$(a_{ij})=\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}$. $\forall\, x\in R$,有

$$\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}(xE_{ij})=(xE_{ij})\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}.$$

即

$$i\text{行}\begin{pmatrix} \cdots & \cdots & \overset{j\text{列}}{\vdots} & \cdots \\ & & ax & \\ & & \vdots & \\ & & \vdots & \end{pmatrix}=\begin{pmatrix} \cdots & \cdots & \overset{j\text{列}}{\vdots} & \cdots \\ & & xa & \\ & & \vdots & \\ & & \vdots & \end{pmatrix}i\text{行}$$

从而 $ax=xa$,所以$(a_{ij})\in\left\{\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}\middle|\, a\in R,\forall\, x\in R,ax=xa\right\}$. 反之,

$\forall\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}$,$a\in R$,$\forall\, x\in R$,$ax=xa$. $\forall\,(b_{ij})\in M_n(R)$,有

$$\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}(b_{ij})=(ab_{ij})=(b_{ij}a)=(b_{ij})\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}.$$

所以$\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}\in Z$. 于是

$$Z=\left\{\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}\middle|\, a\in R,\forall\, x\in R,ax=xa\right\}.$$

8. 证 1),2)略.

3) $\forall a\in Z(S_2)$. $\forall y\in S_1$. 因 $S_1\subset S_2$,故 $y\in S_2$,从而 $ay=ya$,于是 $a\in Z(S_1)$. 所以 $Z(S_2)\subset Z(S_1)$.

4) 设 a 是 R 的任一幂等元,则 $a^2=a$(见第九章,四,12). $\forall x\in R$,

$$\begin{aligned}(axa-ax)^2 &= axaaxa-axaxa-axaax+axax\\ &= axaxa-axaxa-axax+axax=0.\end{aligned}$$

因已知 R 没有非零幂零元,故 $axa=ax$. 同理,$axa=xa$,从而 $ax=xa$. 所以 a 在 R 的中心里.

注 1) 设 $A=\begin{pmatrix}a_1&&&\\&a_2&&\\&&\ddots&\\&&&a_n\end{pmatrix}\in M_n(\mathbb{Q})$,矩阵 A 中主对角线外的元素都是 0,其中 $a_i\neq a_j$,$i\neq j$ 时. 则元 A 在 $M_n(\mathbb{Q})$内的中心化子

$$Z(A)=\left\{\begin{pmatrix}c_1&&&\\&c_2&&\\&&\ddots&\\&&&c_n\end{pmatrix}\middle|\, c_i\in\mathbb{Q}\text{,矩阵中主对角线外的元素都是 0.}\right\}.$$

事实上,$\forall (c_{ij})\in Z(A)$,有

$$(c_{ij})\begin{pmatrix}a_1&&&\\&a_2&&\\&&\ddots&\\&&&a_n\end{pmatrix}=\begin{pmatrix}a_1&&&\\&a_2&&\\&&\ddots&\\&&&a_n\end{pmatrix}(c_{ij}).$$

即$(c_{ij}a_j)=(a_ic_{ij})$,从而左右两个矩阵的(i,j)元相等,即$c_{ij}a_j=a_ic_{ij}$,$(a_i-a_j)C_{ij}=0$. 已知 $i\neq j$ 时,$a_i\neq a_j$,从而 $c_{ij}=0$. 于是$(c_{ij})=\begin{pmatrix}c_{11}&&&\\&c_{22}&&\\&&\ddots&\\&&&c_{nn}\end{pmatrix}$. 反之,$\forall\begin{pmatrix}c_1&&&\\&c_2&&\\&&\ddots&\\&&&c_n\end{pmatrix}$,有

$$\begin{pmatrix}a_1&&&\\&a_2&&\\&&\ddots&\\&&&a_n\end{pmatrix}\begin{pmatrix}c_1&&&\\&c_2&&\\&&\ddots&\\&&&c_n\end{pmatrix}=\begin{pmatrix}a_1c_1&&&\\&a_2c_2&&\\&&\ddots&\\&&&a_nc_n\end{pmatrix}=\begin{pmatrix}c_1a_1&&&\\&c_2a_2&&\\&&\ddots&\\&&&c_na_n\end{pmatrix}=\begin{pmatrix}c_1&&&\\&c_2&&\\&&\ddots&\\&&&c_n\end{pmatrix}\begin{pmatrix}a_1&&&\\&a_2&&\\&&\ddots&\\&&&a_n\end{pmatrix}.$$

于是$\begin{pmatrix}c_1&&&\\&c_2&&\\&&\ddots&\\&&&c_n\end{pmatrix}\in Z(A)$. 所以

$$Z(A)=\left\{\begin{pmatrix}c_1&&&\\&c_2&&\\&&\ddots&\\&&&c_n\end{pmatrix}\middle|\, c_i\in\mathbb{Q}\right\}.$$

2) 设$S=\left\{\begin{pmatrix}a & b\\0 & c\end{pmatrix}\middle| a,b,c\in\mathbb{Z}\right\}\subset M_2(\mathbb{Z})$. 则集$S$在$M_2(\mathbb{Z})$内的中心化子

$$Z(S)=\left\{\begin{pmatrix}a & \\ & a\end{pmatrix}\middle| a\in\mathbb{Z}\right\}.$$

事实上，$\forall\begin{pmatrix}s & t\\u & v\end{pmatrix}\in Z(S)$，$\begin{pmatrix}a_1 & \\ & a_2\end{pmatrix}\in S$，

$$\begin{pmatrix}s & t\\u & v\end{pmatrix}\begin{pmatrix}a_1 & \\ & a_2\end{pmatrix}=\begin{pmatrix}a_1 & \\ & a_2\end{pmatrix}\begin{pmatrix}s & t\\u & v\end{pmatrix}.$$

由本题注1)知$\begin{pmatrix}s & t\\u & v\end{pmatrix}=\begin{pmatrix}d_1 & \\ & d_2\end{pmatrix}$. 又

$$\begin{pmatrix}d_1 & \\ & d_2\end{pmatrix}\begin{pmatrix}a & b\\0 & c\end{pmatrix}=\begin{pmatrix}a & b\\0 & c\end{pmatrix}\begin{pmatrix}d_1 & \\ & d_2\end{pmatrix}.$$

即

$$\begin{pmatrix}d_1a & d_1b\\0 & d_2c\end{pmatrix}=\begin{pmatrix}d_1a & d_2b\\0 & d_2c\end{pmatrix}.$$

从而$d_1b=d_2b$，即$(d_1-d_2)b=0$. 因b是任意整数，故$d_1=d_2\overset{令}{=\!=}d$，所以$\begin{pmatrix}s & t\\u & v\end{pmatrix}=\begin{pmatrix}d_1 & \\ & d_2\end{pmatrix}=\begin{pmatrix}d & \\ & d\end{pmatrix}$. 反之，显然$\begin{pmatrix}a & \\ & a\end{pmatrix}$与$S$中任一元可换. 所以

$$Z(S)=\left\{\begin{pmatrix}a & \\ & a\end{pmatrix}\middle| a\in\mathbb{Z}\right\}.$$

9. 证 利用模5的剩余类环$\mathbb{Z}_5$的加法与乘法的运算表(第九章，四，3)，容易验证映射

$$\phi:[0]\to x,[1]\to y,[2]\to z,[3]\to u,[4]\to v$$

是$\mathbb{Z}_5$与A对于一对加法以及一对乘法来说的同构映射. 因$\mathbb{Z}_5$是环，故A也是环[①].

10. 证 规定$\phi:a\to 1-a$. 显然ϕ是$(R,+,\cdot)$与$(R,\oplus,\odot)$间的一个一一映射. $\forall a,b\in(R,+,\cdot)$，

$$\phi(a)\oplus\phi(b)=(1-a)+(1-b)-1=1-(a+b)=\phi(a+b),$$

$$\begin{aligned}\phi(a)\odot\phi(b)&=(1-a)+(1-b)-(1-a)(1-b)\\&=1-a+1-b-(1-a-b+ab)\\&=1-ab=\phi(ab).\end{aligned}$$

所以$(R,+,\cdot)\overset{\phi}{\cong}(R,\oplus,\odot)$.

11. 证 (反证法)假定ϕ是环R_1与环R_2间的一个同构映射. 则$\phi(1)=1$[②]，从而$\phi(2)=\phi(1+1)=\phi(1)+\phi(1)=1+1=2$. 设$\phi(\sqrt{2})=x$，则$\phi(2)=\phi(\sqrt{2}\cdot\sqrt{2})=\phi(\sqrt{2})\phi(\sqrt{2})=x^2$. 由$\phi$是映射，$x^2=2$，从而$x=\pm\sqrt{2}\,\overline{\in}\,R_2$，产生矛盾. 所以环$R_1$与环$R_2$间没有同构映射.

12. 证 显然，$\phi:a\to a^p$是R到R的一个映射. $\forall a,b\in R$，若$a^p=b^p$，则$a^p-b^p=0$，由

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 98，定理1.

② 同上. 98. 定理2.

第十章，三，4，1）知 $a^p-b^p=(a-b)^p=0$. 因 R 无零因子，故 $a-b=0$，即 $a=b$. 所以ϕ是单射. $\forall a,b\in R$，由 R 是交换环，有

$$\phi(a+b)=(a+b)^p=a^p+b^p=\phi(a)+\phi(b).$$

$$\phi(ab)=(ab)^p=a^pb^p=\phi(a)\phi(b).$$

于是ϕ是 R 的单射的自同态.

注 该ϕ未必是 R 的自同构. 例，$\phi: f(x)\rightarrow\big(f(x)\big)^p$ 是 $\mathbb{Z}_p[x]$的单射的自同态，但 $x(\in\mathbb{Z}_p[x])$在ϕ下无逆象. 若 F 是特征为素数 p 的有限域，则$\phi: a\rightarrow a^p$ 是 F 的自同构. 事实上，ϕ是 F 的单射的自同态. 因 F 是有限域，故由第二章，三，4 鸽笼定理知ϕ是满射. 从而ϕ是 F 的自同构.

13. 证 显然 $F^p\subset F$. 因域 F 有单位元 $1\neq0$，故 $1^p=1(\neq0)\in F^p$. $\forall a^p,b^p\in F^p$，由第十章，三，4，1），

$$a^p-b^p=(a-b)^p\in F^p.$$

$\forall a^p,b^p\in F^p, b^p\neq0$，有

$$a^p(b^p)^{-1}=a^p(b^{-1})^p=(ab^{-1})^p\in F^p.$$

所以 F^p 是 F 的子域.

14. 证 1) ϕ是映射. $\forall f\in E$，$\exists\,|\,(a_{ij})_n\in M_n(\mathbb{Z})$，使得$\varnothing: f\rightarrow(a_{ij})_n$.

2) ϕ是满射. $\forall(b_{ij})_n\in M_n(\mathbb{Z})$. 取

$$g:(s_1,s_2,\cdots,s_n)=\sum_{i=1}^n s_ie_i\rightarrow\sum_{i=1}^n s_i\sum_{j=1}^n b_{ji}e_j.$$

则 g 是G 的一个自同态. 事实上，显然 g 是映射，又 $\forall(s_1,s_2,\cdots,s_n),(t_1,t_2,\cdots,t_n)\in G$，

$$g:(s_1,s_2,\cdots,s_n)=\sum_{i=1}^n s_ie_i\rightarrow\sum_{i=1}^n s_i\sum_{j=1}^n b_{ji}e_j.$$

$$(t_1,t_2,\cdots,t_n)=\sum_{i=1}^n t_ie_i\rightarrow\sum_{i=1}^n t_i\sum_{j=1}^n b_{ji}e_j.$$

于是

$$g:(s_1,s_2,\cdots,s_n)+(t_1,t_2,\cdots,t_n)=(s_1+t_1,s_2+t_2,\cdots,s_n+t_n)=\sum_{i=1}^n(s_i+t_i)e_i$$

$$\rightarrow\sum_{i=1}^n(s_i+t_i)\sum_{j=1}^n b_{ji}e_j=\sum_{i=1}^n s_i\sum_{j=1}^n b_{ji}e_j+\sum_{i=1}^n t_i\sum_{j=1}^n b_{ji}e_j.$$

从而 g 是G 的一个自同态，即 $g\in E$，且

$$g(e_i)=g(0e_1+\cdots+0e_{i-1}+1e_i+0e_{i+1}+\cdots+0e_n)=\sum_{j=1}^n b_{ji}e_j,$$

$i=1,2,\cdots,n$. 所以$\phi: g\rightarrow(b_{ij})_n$.

3) ϕ是单射. $\forall f,g\in E,\phi: f\rightarrow(a_{ij})_n, g\rightarrow(b_{ij})_n$. 若$(a_{ij})_n=(b_{ij})_n$，即 $f(e_i)=g(e_i)$，$i=1,2,\cdots,n$. $\forall(s_1,s_2,\cdots,s_n)\in G$，有$(s_1,s_2,\cdots,s_n)=\sum_{i=1}^n s_ie_i$. 从而

$$f((s_1,s_2,\cdots,s_n))=f(\sum_{i=1}^n s_ie_i)=\sum_{i=1}^n f(s_ie_i)=\sum_{i=1}^n s_if(e_i).$$

同理，

$$g((s_1,s_2,\cdots,s_n))=\sum_{i=1}^n s_i g(e_i).$$

令 $f(e_i)=g(e_i)$，于是 $f((s_1,s_2,\cdots,s_n))=g((s_1,s_2,\cdots,s_n))$，所以 $f=g$.

4) $\forall f,\ g\in E,\phi:f\to(a_{ij})_n,\ g\to(b_{ij})_n$，即

$$f(e_i)=\sum_{j=1}^n a_{ji}e_j,\quad g(e_i)=\sum_{j=1}^n b_{ji}e_j.$$

于是

$$(f+g)(e_i)=f(e_i)+g(e_i)=\sum_{j=1}^n a_{ji}e_j+\sum_{j=1}^n b_{ji}e_j=\sum_{j=1}^n(a_{ji}+b_{ji})e_j,$$

从而

$$\phi:\ f+g\to(a_{ij}+b_{ij})_n=(a_{ij})_n+(b_{ij})_n.$$

又

$$(fg)(e_i)=f(g(e_i))=f(\sum_{j=1}^n b_{ji}e_j)=\sum_{j=1}^n b_{ji}f(e_j)$$

$$=\sum_{j=1}^n b_{ji}\sum_{k=1}^n a_{kj}e_k=\sum_{k=1}^n\sum_{j=1}^n a_{kj}b_{ji}e_k=\sum_{k=1}^n c_{ki}e_k,$$

其中 $c_{ki}=\sum_{j=1}^n a_{kj}b_{ji}$，因此，$c_{ik}=\sum_{j=1}^n a_{ij}b_{jk},i,k=1,2,\cdots,n$. 从而

$$\phi:fg\to(c_{ik})_n=(a_{ij})_n\cdot(b_{ij})_n.$$

综上可知，$E\overset{\phi}{\cong}M_n(\mathbf{Z})$.

15. 解 设ϕ是$\mathbf{Z}_2$到$\mathbf{Z}$的任一同态映射，则由第十一章，三，3，1)，$\phi([0])=0$. 又

$$\phi([1])+\phi([1])=\phi([1]+[1])=\phi([2])=\phi([0])=0,$$

从而 $2\phi([1])=0$，即$\phi([1])=0$. 因此$\mathbf{Z}_2$到$\mathbf{Z}$的同态映射只有一个零同态：$\phi=0$(见第十一章，四，3，2)).

16. 证 ϕ_1与ϕ_2显然是使$\forall a\in\mathbf{R},a\to\begin{pmatrix}a&0\\0&a\end{pmatrix}$的 $\mathbf{C}$与M间的同构映射.

若ϕ是任一个使$\forall a\in\mathbf{R},a\to\begin{pmatrix}a&0\\0&a\end{pmatrix}$的$\mathbf{C}$与$M$间的同构映射. 设$\phi(\mathrm{i})=\begin{pmatrix}a&b\\-b&a\end{pmatrix}$，则

$\phi(\mathrm{i}^2)=\begin{pmatrix}a&b\\-b&a\end{pmatrix}^2$，即

$$\phi(-1)=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}=\begin{bmatrix}a^2-b^2&2ab\\-2ab&a^2-b^2\end{bmatrix}.$$

从而 $a^2-b^2=-1$ 且 $ab=0$. 解之，得 $a=0,b=\pm1$. 当 $a=0,b=1$ 时，$\phi(\mathrm{i})=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$，此时 $\forall a+b\mathrm{i}\in\mathbf{C}$，

$$\phi(a+b\mathrm{i})=\phi(a)+\phi(b)\,\phi(\mathrm{i})=\begin{pmatrix}a&0\\0&a\end{pmatrix}+\begin{pmatrix}b&0\\0&b\end{pmatrix}\begin{pmatrix}0&1\\-1&0\end{pmatrix}=\begin{pmatrix}a&b\\-b&a\end{pmatrix}$$

$$=\phi_1(a+b\mathrm{i}).$$

即$\phi=\phi_1$；当 $a=0,b=-1$ 时，$\phi(\mathrm{i})=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$，此时$\forall a+b\mathrm{i}\in\mathbf{C}$，

$$\phi(a+bi)=\phi(a)+\phi(b)\,\phi(i)=\begin{pmatrix}a&0\\0&a\end{pmatrix}+\begin{pmatrix}b&0\\0&b\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}=\begin{pmatrix}a&-b\\b&a\end{pmatrix}$$
$$=\phi_2(a+bi).$$

即$\phi=\phi_2$.

所以命题得证.

17. 解 1) $[1]x^4+[1]x^3-[1]x^2-[1]x+[1]=x^4+x^3-x^2-x+1$.

2)

$$\begin{array}{rl} & x_1+x_2\qquad +x_4=1\\ 1 & \qquad x_2+x_3+x_4=0\\ \hline & x_1\qquad -x^3\qquad =1\end{array}$$

$$\begin{array}{r} x_1-x_3=1\\ +x_1+x_3=1\\ \hline [2]x_1\qquad=[2]\end{array}$$

从而 $x_1=1$. 代入 $x_1-x_3=1$,得 $x_3=0$. 代入 $x_2+x_3+x_4=0$,得 $x_2=-x_4$. 因此方程组的解是:

$$x_1=1,x_2=-x_4,x_3=0,x_4=x_4.$$

所以方程组的所有解是:

$$\begin{cases}x_1=1\\x_2=0\\x_3=0\\x_4=0,\end{cases}\qquad\begin{cases}x_1=1\\x_2=[2]\\x_3=0\\x_4=1,\end{cases}\qquad\begin{cases}x_1=1\\x_2=1\\x_3=0\\x_4=[2].\end{cases}$$

18. 证 显然ψ是$M_n(R)$到$M_n(\overline{R})$的一个映射. $\forall\,(a_{ij}),(b_{ij})\in M_n(R)$,

$$\psi[(a_{ij})+(b_{ij})]=\psi[(a_{ij}+b_{ij})]=(\overline{a_{ij}+b_{ij}})=(\phi(a_{ij}+b_{ij}))$$
$$=(\phi(a_{ij})+\phi(b_{ij}))=(\overline{a_{ij}}+\overline{b_{ij}})=(\overline{a_{ij}})+(\overline{b_{ij}})$$
$$=\psi(a_{ij})+\psi(b_{ij}).$$

$$\psi[(a_{ij})(b_{ij})]=\psi\left(\sum_{k=1}^{n}a_{ik}b_{kj}\right)=\left(\overline{\sum_{k=1}^{n}a_{ik}\,b_{kj}}\right)$$
$$=\left(\phi\left(\sum_{k=1}^{n}a_{ik}b_{kj}\right)\right)=\left(\sum_{k=1}^{n}\bar{a}_{ik}\,\bar{b}_{kj}\right)=\left(\overline{a_{ij}}\right)\left(\overline{b_{ij}}\right)$$
$$=\psi(a_{ij})\cdot\psi(b_{ij}).$$

所以ψ是$M_n(R)$到$M_n(\overline{R})$的一个同态映射.

19. 证 1) ϕ是F到F的一个单射. 事实上, $\forall\,x,y\in F$,若$\phi(x)=\phi(y)$,则

$$\phi(x-y)=\phi(x+(-y))=\phi(x)+\phi(-y)=\phi(x)+(-\phi(y))=\phi(x)-\phi(y)=0.$$

若 $x-y\neq0$,则由已知$\phi(x-y)\cdot\phi[(x-y)^{-1}]=1$,但其中$\phi(x-y)=0$,产生矛盾. 从而 $x-y=0$,即 $x=y$. 因此ϕ是单射.

所以ϕ是F与F间的一个一一映射.

2) 先证明$\phi(x^2)=(\phi(x))^2$. 因

$$x(x-1)[(x-1)^{-1}-x^{-1}]=x(x-1)(x-1)^{-1}-x(x-1)x^{-1}$$
$$=x-xxx^{-1}+xx^{-1}=x-x+1=1.$$

故$[(x-1)^{-1}-x^{-1}]^{-1}=x(x-1)=x^2-x$，即

$$x^2=[(x-1)^{-1}-x^{-1}]^{-1}+x.$$

从而

$$\begin{aligned}
\phi(x^2) &= \phi([(x-1)^{-1}-x^{-1}]^{-1}+x) \\
&= \phi([(x-1)^{-1}-x^{-1}]^{-1})+\phi(x) \\
&= \left[\phi\left((x-1)^{-1}-x^{-1}\right)\right]^{-1}+\phi(x) \quad (\text{由已知}\phi(x^{-1})=(\phi(x))^{-1}) \\
&= \left\{\left[\phi(x-1)\right]^{-1}-\left[\phi(x)\right]^{-1}\right\}^{-1}+\phi(x) \\
&= \left\{\left[\phi(x)-\phi(1)\right]^{-1}-\left[\phi(x)\right]^{-1}\right\}^{-1}+\phi(x) \\
&= \left\{\left[\phi(x)-1\right]^{-1}-\left[\phi(x)\right]^{-1}\right\}^{-1}+\phi(x) \\
&= \left[\phi(x)\right]^2-\phi(x)+\phi(x) \quad (\text{理由与}\left[(x-1)^{-1}-x^{-1}\right]^{-1}=x^2-x\text{同}) \\
&= \left[\phi(x)\right]^2.
\end{aligned}$$

3) $\forall x,y\in F$，有

$$\phi\left((x+y)^2\right)=\phi(x^2+2xy+y^2)=\phi(x^2)+2\,\phi(xy)+\phi(y^2).$$

又

$$\begin{aligned}
\phi\left((x+y)^2\right) &= \left[\phi(x+y)\right]^2=\left[\phi(x)+\phi(y)\right]^2 \\
&= \left(\phi(x)\right)^2+2\,\phi(x)\,\phi(y)+\left[\phi(y)\right]^2=\phi(x^2)+2\,\phi(x)\,\phi(y)+\phi(y^2).
\end{aligned}$$

从而$2\,\phi(xy)=2\,\phi(x)\phi(y)$，即$2\left[\phi(xy)-\phi(x)\phi(y)\right]=0$. 于是$\phi(xy)-\phi(x)\phi(y)=0$. 否则，若$\phi(xy)-\phi(x)\phi(y)\neq 0$，则由已知，$2\left[\phi(xy)-\phi(x)\phi(y)\right]\neq 0$，产生矛盾. 因此$\phi(xy)=\phi(x)\phi(y)$.

综上可知，ϕ是域F的一个自同构.

第十二章

1. 解 1) S是$\mathbf{R}[x,y]$的理想. 由定义可证.

2) S不是$\mathbf{R}[x,y]$的理想. 因取$x\in\mathbf{R}[x,y]$，$y\in S$，但$xy\,\overline{\in}\,S$.

3) S是$\mathbf{R}[x,y]$的理想. 由定义可证.

4) S不是$\mathbf{R}[x,y]$的理想. 因取$x\in\mathbf{R}[x,y]$，$x\in S$，但$xx=x^2\,\overline{\in}\,S$.

2. 证 1) 因$\mathfrak{A}$是R的理想，故$0=0^1\in\mathfrak{A}$，从而$0\in S$，即$S\neq\Phi$. 显然$S\subset R$. $\forall a,b\in S$. $\exists$正整数n,m，使得$a^n,b^m\in\mathfrak{A}$. 因R是交换环，故由第九章，二，3，

$$(a-b)^{m(n+1)}=a^{m(n+1)}-C^1_{m(n+1)}a^{m(n+1)-1}b+\cdots+(-1)^iC^i_{m(n+1)}a^{m(n+1)-i}b^i+\cdots+(-1)^{m(n+1)}b^{m(n+1)}.$$

当$i<m$时，$m(n+1)-i>m(n+1)-m=mn\geqslant n$，从而$m(n+1)-i-n$是正整数. 又因$a^n\in\mathfrak{A}$，$\mathfrak{A}$是$R$的理想，故

$$(-1)^iC^i_{m(n+1)}a^{m(n+1)-i}b^i=(-1)^iC^i_{m(n+1)}a^{m(n+1)-i-n}\cdot a^n\cdot b^i\in\mathfrak{A}.$$

当$i\geqslant m$时，$i-m$是非负整数. 又因$b^m\in\mathfrak{A}$，$\mathfrak{A}$是R的理想，故

$$(-1)^i C_{m(n+1)}^i a^{m(n+1)-i} b^i = (-1)^i C_{m(n+1)}^i a^{m(n+1)-i} \cdot b^m \cdot b^{i-m} \in \mathfrak{A}.$$

由$\mathfrak{A}$是加群，$(a-b)^{m(n+1)}\in\mathfrak{A}$. 于是$a-b\in S$. $\forall r\in R, a\in S$，$\exists$正整数n，使得$a^n\in\mathfrak{A}$. 因R是交换环，$\mathfrak{A}$是R的理想，故$(ra)^n=r^n a^n\in\mathfrak{A}$，从而$ra\in S$. 同理，$ar\in S$. 所以$S$是$R$的理想.

2)　$\forall x\in\mathfrak{A}$，$\exists$正整数1，使得$x^1=x\in\mathfrak{A}$，从而$x\in S$，所以$\mathfrak{A}\subset S$.

3)　与2)同理可证.

4)　($\Rightarrow$)　因R有单位元1，故由$S=R$，$1\in S$，即$\exists$正整数n，使得$1^n=1\in\mathfrak{A}$. 又$\mathfrak{A}$是R的理想，从而由第十二章，一，4，10)知$\mathfrak{A}=R$.

($\Leftarrow$)　显然$S\subset R$；反之，$\forall r\in R$，由$R=\mathfrak{A}$，$r=\mathfrak{A}$，由本题2)，$\mathfrak{A}\subset S$，从而$\gamma\in S$，即$R\subset S$. 所以$S=R$.

注　若$R=\mathbb{Z}$，$\mathfrak{A}=(4)$，$S=\{x\in\mathbb{Z}\mid\exists$正整数$n$，使得$x^n\in(4)\}$，则$S=(2)$. 事实上，$\forall x\in S$，都有正整数$n$，使得$x^n\in(4)$. 从而$4\mid x^n$，即$2\mid x^n$. 因2是素数，故$2\mid x$，于是$x\in(2)$，因此$S\subset(2)$；反之，$\forall 2q\in(2)$，$(2q)^2=4q^2\in(4)$，于是$2q\in S$，因此$(2)\subset S$，所以$(2)=S$.

3. 证　由定义易证S是R的左理想. 因R有单位元1，故

$$a_i = 0a_1 + \cdots + 0a_{i-1} + 1a_i + 0a_{i+1} + \cdots + 0a_n \in S.$$

若S_1是含$a_1,a_2,\cdots,a_n$的R的任一左理想. $\forall \sum_{i=1}^n x_i a_i\in S$，因$S_1$是左理想，故$x_i a_i\in S_1$，因$S_1$是加群，故$\sum_{i=1}^n x_i a_i\in S_1$，从而$S\subset S_1$. 所以$S$是含$a_1,a_2,\cdots,a_n$的$R$的最小左理想.

注　该命题给出由有单位元的环中的n个元构造出R的最小左理想的方法.

4. 证　略.

注　1)　由第十二章，三，1，3)知，当R是交换环时，S是R的理想；但当R不是交换环时，S未必是R的理想. 例，取定$\begin{pmatrix}0&0\\0&1\end{pmatrix}\in$环$M_2(\mathbb{Q})$，则

$$\begin{aligned}S&=\left\{\begin{pmatrix}x&y\\u&v\end{pmatrix}\in M_2(\mathbb{Q})\,\middle|\,\begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix}x&y\\u&v\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}\right\}\\&=\left\{\begin{pmatrix}x&y\\u&v\end{pmatrix}\in M_2(\mathbb{Q})\,\middle|\,\begin{pmatrix}0&0\\u&v\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}\right\}\\&=\left\{\begin{pmatrix}x&y\\u&v\end{pmatrix}\in M_2(\mathbb{Q})\,\middle|\,u=v=0\right\}=\left\{\begin{pmatrix}x&y\\0&0\end{pmatrix}\,\middle|\,x,y\in\mathbb{Q}\right\}\end{aligned}$$

是$M_2(\mathbb{Q})$的一个右理想，但不是$M_2(\mathbb{Q})$的理想(见第十二章，二，6，注1)).

2)　取定$a\in$环R，则$T=\{x\in R\mid xa=0\}$是R的左理想.

5. 证　由$0\in R$且$0R=\{0\}\subset S$，$0\in\mathfrak{A}$，即$\mathfrak{A}\neq\Phi$. 显然$\mathfrak{A}\subset R$. $\forall x,y\in\mathfrak{A}$，有$x,y\in R$，$xR\subset S$，$yR\subset S$. 因此$x-y\in R$. 又

$$(x-y)R=\{(x-y)r\mid r\in R\}=\{xr-yr\mid r\in R\}.$$

$\forall xr-yr\in(x-y)R$，因$xR\subset S$，$yR\subset S$，故$xr,yr\in S$，又S是加群，从而$xr-yr\in S$，于是$(x-y)R\subset S$，所以$x-y\in\mathfrak{A}$. $\forall a\in R$，$x\in\mathfrak{A}$，有$x\in R$，$xR\subset S$. 又因S是R的左理想，故$(ax)R$

$=a(xR)\subset aS\subset S$，所以 $ax\in\mathfrak{A}$. 同理 $xa\in\mathfrak{A}$. 因此$\mathfrak{A}$是 R 的理想.

6. 证 1） 由第九章，四，12，6），

a 是环 R 的幂零元$\Leftrightarrow\exists$正整数 n，使得 $a^n=0$，且交换环 R 中所有幂零元的集$\mathfrak{A}$作成一个环. $\forall r\in R$，$\forall a\in\mathfrak{A}$，$\exists$正整数 n，使得 $a^n=0$，再由 R 是交换环，有$(ra)^n=r^na^n=r^n0=0$，从而 $ra\in\mathfrak{A}$. 同理 $ar\in\mathfrak{A}$. 所以$\mathfrak{A}$是 R 的理想.

2） 若$[x]$是 $R/\mathfrak{A}$中的一个幂零元，则$\exists$正整数 n，使得$[x]^n=[0]$，即$[x^n]=[0]$，从而 $x^n\in\mathfrak{A}$. 于是$\exists$正整数 k，使得$(x^n)^k=x^{nk}=0$，因此 $x\in\mathfrak{A}$. 所以$[x]=x+\mathfrak{A}=\mathfrak{A}=[0]$. 从而 $R/\mathfrak{A}$中只有零元$[0]$是幂零元.

7. 证 1）因 $S0=\{0\}$，故 $0\in\mathfrak{A}$，即$\mathfrak{A}\neq\Phi$. 显然$\mathfrak{A}\subset R$. $\forall x,y\in\mathfrak{A}$，$Sx=Sy=\{0\}$，即$\forall s\in S$，$sx=sy=0$，从而 $s(x-y)=sx-sy=0-0=0$，于是 $S(x-y)=\{0\}$，因此 $x-y\in\mathfrak{A}$. $\forall r\in R$，$x\in\mathfrak{A}$，由 $Sx=\{0\}$及 S 是 R 的右理想知：

$$S(xr)=(Sx)r=\{0\}r=\{0\},\ S(rx)=(Sr)x\subset Sx=\{0\}.$$

即 $S(rx)=\{0\}$. 从而 $xr,rx\in\mathfrak{A}$. 所以$\mathfrak{A}$是 R 的理想.

2） 与 1）类似可证.

注 1） 将该命题中的 S 特别取成环 R 时，$\mathfrak{A}=\left\{x\in R\,\middle|\,Rx=\{0\}\right\}$是 R 的理想且是 R 的右零化子.

2） 由第十一章，三，8 的证明知：设 R 是环，取定 $a\in R$，$f_a:x\to ax$ 是加群 R 的一个自同态. 作集 $\overline{E}=\left\{f_a\,\middle|\,a\in R\right\}$，则 $\overline{E}$ 是一个自同态环，且$\phi:a\to f_a$ 是环 R 到环 $\overline{E}$ 的一个同态满射. 于是

$$\ker\phi=\left\{b\in R\,\middle|\,f_b=0\right\}=\left\{b\in R\,\middle|\,\forall x\in R,bx=0\right\}=\left\{b\in R\,\middle|\,bR=\{0\}\right\}$$

是 R 的左零化子. 当 R 有单位元 1 时，$\forall b\in\ker\phi$，有 $b\cdot 1=0$，从而 $b=0$，因此 $\ker\phi=\{0\}$. 由第十二章，二，8，$R\overset{\phi}{\cong}\overline{E}$.

3） 由第十二章，三，1，9）知，$S=\left\{(0,y)\,\middle|\,y\in\mathbf{Z}\right\}$是环 $R=\left\{(x,y)\,\middle|\,x,y\in\mathbf{Z}\right\}$的一个理想，则 S 在 R 中的左零化子是

$$\mathfrak{A}=\left\{(x,y)\in R\,\middle|\,(x,y)S=\left\{(0,0)\right\}\right\}=\left\{(x,0)\,\middle|\,x\in\mathbf{Z}\right\}.$$

事实上，$\forall(x,y)\in\mathfrak{A}$，$(x,y)S=\left\{(0,0)\right\}$，从而取$(0,1)\in S$，有$(x,y)(0,1)=(0,y)=(0,0)$，即 $y=0$，于是$(x,y)=(x,0)$. 因此$\mathfrak{A}\subset\left\{(x,0)\,\middle|\,x\in\mathbf{Z}\right\}$；反之，$\forall(x,0)\in\left\{(x,0)\,\middle|\,x\in\mathbf{Z}\right\}$，有$(x,0)S=\left\{(0,0)\right\}$，从而$(x,0)\in\mathfrak{A}$，因此$\left\{(x,0)\,\middle|\,x\in\mathbf{Z}\right\}\subset\mathfrak{A}$. 所以$\mathfrak{A}=\left\{(x,0)\,\middle|\,x\in\mathbf{Z}\right\}$.

8. 证 若 $R=\{0\}$，则 R 是幂零元环.

若 $R\neq\{0\}$. 任意取 $a\in R$，$Ra=\left\{ra\,\middle|\,r\in R\right\}$是 R 的左理想（见第十二章，二，6，注 4））. 由题设 $Ra=R$ 或 $Ra=\{0\}$.

1） 如果$\exists a(\neq 0)\in R$，使得 $Ra=\{0\}$，那么$\mathfrak{A}=\left\{x\,\middle|\,Rx=\{0\}\right\}\neq\{0\}$. 由上题注 1），$\mathfrak{A}$是 R 的理想. 再由题设，$\mathfrak{A}=R$. 从而$\forall r\in R$，有 $r\in\mathfrak{A}$，即 $Rr=\{0\}$，因此 $r\cdot r=r^2=0$，于是 r 是幂零元. 所以 R 是幂零元环.

2） 如果$\forall a(\neq 0)\in R$，使得 $Ra\neq\{0\}$，那么 $Ra=R$. 即$\forall a(\neq 0)$，$b\in R$，方程 $ya=b$ 在

R 中有解. 由第十章,三,3 知 R 是除环.

注 1) 将该命题中的左理想改为右理想,命题仍成立.

2) 可将原命题改为:设 R 是环,且 $R^2\neq\{0\}$,则 R 的左理想只有 R 和 $\{0\}\Leftrightarrow R$ 是除环. 事实上,($\Rightarrow$) 由原命题的证明可知 R 只能是除环. ($\Leftarrow$) 由第十二章,一,4,3)可知结论.

3) 还可将原命题改为:设 R 是有单位元 $1(\neq0)$的环,则

$$R\text{ 的左理想只有 }R\text{ 和}\{0\}\Leftrightarrow R\text{ 是除环.}$$

事实上,($\Rightarrow$) 因 R 的单位元 $1\neq0$,故 R 中有非零元. $\forall a(\neq0)\in R, Ra=\{ra\mid r\in R\}$是 R 的左理想. 因 R 有单位元 1,故 $a=1a\in Ra$,从而 $Ra\neq\{0\}$. 由题设 $Ra=R$. 与原命题证明中的 2)同样可知 R 是除环. ($\Leftarrow$) 同注 2).

4) 若 R 是有单位元 $1(\neq0)$的环,R 的左理想只有 R 和$\{0\}$,由注 3)知 R 是除环. 由第十一章,二,2 知,R 的中心是域.

9. 证 1) $\forall r\in R$,因 $e\in Z$,故

$$r(1-e)=r-re=r-er=(1-e)r,$$

从而 $1-e\in Z$.

2) 因 $e^2=e$,故

$$(1-e)^2=1-e-e+e^2=1-e-e+e=1-e,$$

从而 $1-e$ 也是幂等元.

3) 由第十二章,二,6,注 4),eR 是 R 的右理想. 又 $\forall r\in R, \forall ea\in eR$,其中 $a\in R$,因 $e\in Z$,故

$$r(ea)=(re)a=(er)a=e(ra)\in eR.$$

从而 eR 是 R 的左理想. 所以 eR 是 R 的理想.

由本题 1)知 $1-e\in Z$,从而$(1-e)R$ 也是 R 的理想.

10. 证 由第十章,三,3,只需证明:$\forall a(\neq0), b\in R$,方程 $ax=b$ 在 R 中有解. 已知 R 有非零元. $\forall a(\neq0)\in R$,因 R 是交换环,故 $Ra, Ra^2, Ra^3, \cdots$都是 R 的理想(见第十二章,二,6,注 4)). 由题设,理想的个数有限,从而必有 $Ra^m=Ra^n$, $m<n$. 于是 $\forall b\in R, \exists c\in R$,使得 $ba^m=ca^n$. 因 R 无零因子,消去律成立,且 $a^m\neq0$,故 $b=ca^{n-m}$. 因 R 可交换,故 $a(a^{n-m-1}c)=b$. 所以,$\forall a(\neq0), b\in R$,方程 $ax=b$ 在 R 中有解 $a^{n-m-1}c$.

11. 解 $\left[([3]x^2-[1]x+[1])+\mathfrak{A}\right]\left[([2]x-[1])+\mathfrak{A}\right]=([1]x^3+[3]x-[1])+\mathfrak{A}$
$=\left[([3]x^2+[3]x+[2])([2]x+[3])+[3]\right]+\mathfrak{A}=[3]+\mathfrak{A}.$

12. 证 $[x+1],[x-1]\in F[x]/(x^2-1)$. 因 $x^2-1\nmid x+1, x^2-1\nmid x-1$,又 $F[x]$是有单位元的交换环,故 $x+1\,\overline{\in}\,(x^2-1), x-1\,\overline{\in}\,(x^2-1)$,从而$[x+1]\neq[0], [x-1]\neq[0]$. 但$[x+1][x-1]=\left[(x+1)(x-1)\right]=[x^2-1]=[0]$. 所以$[x+1]$与$[x-1]$是 $F[x]/(x^2-1)$的零因子.

13. 证 1) $\phi: f(x)\to f(\mathrm{i})$是 $\mathbf{Z}[x]$到 $\mathbf{Z}[\mathrm{i}]$的一个同态满射. 事实上,$\forall f(x)\in\mathbf{Z}[x], \exists! g(x)\in\mathbf{Z}[x], a, b\in\mathbf{Z}$,使得 $f(x)=g(x)(x^2+1)+a+bx$,即 $\exists! a+b\mathrm{i}\in\mathbf{Z}[\mathrm{i}]$,使得$\phi(f(x))=f(\mathrm{i})=g(\mathrm{i})(\mathrm{i}^2+1)+a+b\mathrm{i}=a+b\mathrm{i}$. 因此$\phi$是映射. $\forall a+b\mathrm{i}\in\mathbf{Z}[\mathrm{i}], \exists a+bx\in\mathbf{Z}[x]$,使得$\phi(a+bx)=a+b\mathrm{i}$. 因此$\phi$是满射. $\forall f(x), g(x)\in\mathbf{Z}[x], \phi(f(x)+g(x))=f(\mathrm{i})+$

$g(\mathrm{i})=\phi(f(x))+\phi(g(x))$. $\phi(f(x)g(x))=f(\mathrm{i})g(\mathrm{i})=\phi(f(x))\phi(g(x))$. 所以$\phi$是$\mathbb{Z}[x]$到$\mathbb{Z}[\mathrm{i}]$的一个同态满射.

$\ker\phi=(x^2+1)$. 事实上，$\forall f(x)\in\ker\phi$，$\exists g(x)$，$a+bx\in\mathbb{Z}[x]$，使得 $f(x)=g(x)(x^2+1)+a+bx$. 由$\phi(f(x))=0$，有 $f(\mathrm{i})=g(\mathrm{i})(\mathrm{i}^2+1)+a+b\mathrm{i}=a+b\mathrm{i}=0$，从而 $a=b=0$，于是 $f(x)=g(x)(x^2+1)\in(x^2+1)$. 因此 $\ker\phi\subset(x^2+1)$；反之，$\forall f(x)\in(x^2+1)$，因$\mathbb{Z}[x]$是有单位元的交换环，故$\exists g(x)\in\mathbb{Z}[x]$，使得 $f(x)=g(x)(x^2+1)$，从而$\phi(f(x))=f(\mathrm{i})=g(\mathrm{i})(\mathrm{i}^2+1)=0$，于是 $f(x)\in\ker\phi$. 因此$(x^2+1)\subset\ker\phi$. 所以 $\ker\phi=(x^2+1)$.

由同态基本定理，$\mathbb{Z}[x]/(x^2+1)\cong\mathbb{Z}[\mathrm{i}]$.

注 ① 如果想避开$\mathbb{Z}[x]$中带余除法定理，可如下证明：$\phi: f(x)\to f(\mathrm{i})$是$\mathbb{Z}[x]$到$\mathbb{Z}[\mathrm{i}]$的映射：$\forall f(x)=a_0+a_1x+\cdots+a_nx^n\in\mathbb{Z}[x]$，$f(\mathrm{i})=a_0+a_1\mathrm{i}+\cdots+a_n\mathrm{i}^n$. 因 $\mathrm{i}^{4k}=1$，$\mathrm{i}^{4k+1}=\mathrm{i}$，$\mathrm{i}^{4k+2}=-1$，$\mathrm{i}^{4k+3}=-\mathrm{i}$，其中 k 是任意整数，故 $f(\mathrm{i})=a+b\mathrm{i}$，$a,b\in\mathbb{Z}$. 所以 $\forall f(x)\in\mathbb{Z}[x]$，$\exists|f(\mathrm{i})=a+b\mathrm{i}\in\mathbb{Z}[\mathrm{i}]$，使得$\phi(f(x)=f(\mathrm{i})$. 至于 $\ker\phi\subset(x^2+1)$可如下证明：$\forall f(x)\in\ker\phi$，$\phi(f(x))=f(\mathrm{i})=0$，从而 i 是整系数多项式 $f(x)$的根. 由《高等代数》[①]知，i 的共轭复数$-\mathrm{i}$也是 $f(x)$的根，因此 $x-\mathrm{i}\mid f(x)$，$x+\mathrm{i}\mid f(x)$. 因 $x-\mathrm{i}$ 与 $x+\mathrm{i}$ 互素，且$(x-\mathrm{i})(x+\mathrm{i})=x^2+1$，故 $x^2+1\mid f(x)$，于是$\exists g(x)\in\mathbb{Z}[x]$，使得 $f(x)=g(x)(x^2+1)$. 所以 $f(x)\in(x^2+1)$，即 $\ker\phi\subset(x^2+1)$.

② 还可如下直接证明$\mathbb{Z}[x]/(x^2+1)\cong\mathbb{Z}[\mathrm{i}]$：$\forall f(x)\in\mathbb{Z}[x]$，$\exists|g(x)$，$a+bx\in\mathbb{Z}[x]$，使得 $f(x)=g(x)(x^2+1)+a+bx$，即 $f(x)-(a+bx)=g(x)(x^2+1)\in(x^2+1)$，从而$[f(x)]=[a+bx]$. 所以$\mathbb{Z}[x]/(x^2+1)=\{[a+bx]\mid a,b\in\mathbb{Z}\}$. 于是

$$\psi:[a+bx]\to a+b\mathrm{i}$$

是$\mathbb{Z}[x]/(x^2+1)$与$\mathbb{Z}[\mathrm{i}]$间的同构映射．事实上，

(i) $\forall[a+bx]\in\mathbb{Z}[x]$，$\exists a+b\mathrm{i}\in\mathbb{Z}[\mathrm{i}]$，使得 $\psi([a+bx])=a+b\mathrm{i}$. 若$[a+bx]=[c+dx]$，则$(a+bx)-(c+dx)=(a-c)+(b-d)x\in(x^2+1)$. 但$(x^2+1)$中除零多项式外，都是二次或二次以上的多项式，因此$(a-c)+(b-d)x=0$. 因 x 是$\mathbb{Z}$上未定元，故 $a=c$，$b=d$. 从而 $a+bx=c+dx$. 所以$\forall[a+bx]\in\mathbb{Z}[x]$，$\exists|a+b\mathrm{i}\in\mathbb{Z}[\mathrm{i}]$，使得 $\psi([a+bx])=a+b\mathrm{i}$.

(ii) $\forall a+b\mathrm{i}\in\mathbb{Z}[\mathrm{i}]$，$\exists[a+bx]\in\mathbb{Z}[x]/(x^2+1)$，使得 $\psi([a+bx])=a+b\mathrm{i}$.

(iii) $\forall[a+bx],[c+dx]\in\mathbb{Z}[x]/(x^2+1)$，若 $a+bx=c+dx$，又 x 是$\mathbb{Z}$上未定元，则 $a=c$，$b=d$，从而$[a+bx]=[c+dx]$.

(iv) $\forall[a+bx],[c+dx]\in\mathbb{Z}[x]/(x^2+1)$，

$$\begin{aligned}\psi([a+bx]+[c+dx])&=\psi\big([(a+c)+(b+d)x]\big)=(a+c)+(b+d)\mathrm{i}\\&=(a+b\mathrm{i})+(c+d\mathrm{i})\\&=\psi([a+bx])+\psi([c+dx]).\\\psi\big([a+bx][c+dx]\big)&=\psi\big([ac+(ad+bc)x+bdx^2]\big)\\&=\psi\big([(ac-bd)+(ad+bc)x+bd(x^2+1)]\big)\\&=\psi\big([(ac-bd)+(ad+bc)x]\big)=(ac-bd)+(ad+bc)\mathrm{i}\end{aligned}$$

---

① 北京大学数学系几何与代数教研室. 高等代数. 北京：高等教育出版社，1978.

$$= (a+bi)(c+di) = \psi([a+bx])\psi([c+dx]).$$

所以 $\mathbb{Z}[x]/(x^2+1)\overset{\phi}{\cong}\mathbb{Z}[i]$.

2） 与 1)类似可证ϕ是$\mathbb{R}[x]$到$\mathbb{C}$的一个同态满射. $\ker\phi=(x^2+1)$. $\mathbb{R}[x]/(x^2+1)\cong\mathbb{C}$.

注 $\mathbb{R}[x]$模理想(x^2+1)的剩余类环$\mathbb{R}[x]/(x^2+1)$是与复数域$\mathbb{C}$同样结构的域.

3） 易证ϕ是R到$\mathbb{Z}$的一个同态满射. $\ker\phi=\{(a,b)\in R \mid \phi((a,b))=a=0\}=\{(0,b)\mid b\in\mathbb{Z}\}$. $R/\ker\phi\cong\mathbb{Z}$.

4） 易证ϕ是同态满射. $\ker\phi=\{2n \mid n\in\mathbb{Z}\}=2\mathbb{Z}$. $\mathbb{Z}/\ker\phi\cong\overline{R}$.

5） 易证ϕ是同态满射. $\ker\phi=\{a\in\mathbb{Z} \mid 6\mid 4a\}$. $\mathbb{Z}/\ker\phi\cong\overline{R}$.

6） $\forall\bar{a}\in\mathbb{Z}_m$, $\exists[a]\in\mathbb{Z}_r$, 使得$\phi(\bar{a})=[a]$. 若$\bar{a}=\bar{b}$, 则$m\mid a-b$, 又已知$r\mid m$, 从而$r\mid a-b$, 于是$[a]=[b]$. 所以$\forall\bar{a}\in\mathbb{Z}_m$, $\exists|[a]\in\mathbb{Z}_r$, 使得$\phi(\bar{a})=[a]$. 即$\phi$是映射. 显然$\phi$是满射. $\forall\bar{a},\bar{b}\in\mathbb{Z}_m$, $\phi(\bar{a}+\bar{b})=\phi(\overline{a+b})=[a+b]=[a]+[b]$. 所以$\phi$是$\mathbb{Z}_m$到$\mathbb{Z}_r$的一个同态满射.

$$\ker\phi=\{\bar{a}\in\mathbb{Z}_m \mid \phi(\bar{a})=[a]=[0]\}=\{\bar{a}\in\mathbb{Z}_m \mid r\mid a\}$$
$$=\{\bar{a}\in\mathbb{Z}_m \mid a\in(r)\}=\{a+(m) \mid a\in(r)\}=(r)/(m).$$

$\mathbb{Z}_m/\ker\phi\cong\mathbb{Z}_r$, 即$\mathbb{Z}/(m)/(r)/(m)\cong\mathbb{Z}/(r)$（见第十二章，一，5，4)，注②，例2).

7） 易证ϕ是同态满射. $\ker\phi=\left\{\begin{pmatrix}a&b\\0&c\end{pmatrix} \,\middle|\, \phi\left(\begin{pmatrix}a&b\\0&c\end{pmatrix}\right)=\begin{pmatrix}0&0\\0&0\end{pmatrix}\right\}=\left\{\begin{pmatrix}a&b\\0&c\end{pmatrix} \,\middle|\, \begin{pmatrix}a&0\\0&c\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}\right\}=\left\{\begin{pmatrix}a&b\\0&c\end{pmatrix} \,\middle|\, a=c=0\right\}=\left\{\begin{pmatrix}0&b\\0&0\end{pmatrix} \,\middle|\, b\in\mathbb{Z}\right\}$. $R/\ker\phi\cong\overline{R}$.

8） 易证ϕ是同态满射. $\ker\phi=\left\{\begin{pmatrix}a&b\\0&0\end{pmatrix} \,\middle|\, a,b\in\mathbb{Z}\right\}$. $R/\ker\phi\cong\overline{R}$.

9） 易证ϕ是同态满射. $\ker\phi=\left\{\begin{pmatrix}2a&2b\\2c&2d\end{pmatrix} \,\middle|\, a,b,c,d\in\mathbb{Z}\right\}$. $M_2(\mathbb{Z})/\ker\phi\cong\overline{R}$.

注 因$\mathbb{Z}_2$中的元有且只有$[0]$与$[1]$，故$\overline{R}$中的元有且只有$2^4=16$个，所以$M_2(\mathbb{Z})/\ker\phi$恰含16个元.

10） 易证ϕ是同态满射. $\ker\phi=M_n(\mathfrak{A})$，其中$\mathfrak{A}=\ker\psi$. $M_n(S)/M_n(\mathfrak{A})\cong M_n(\overline{S})$.

11） 易证ϕ是同态满射. $\ker\phi=\left\{\sum_{i=0}^{n}a_ix^i \,\middle|\, a^i\in a\right\}=\mathfrak{A}[x]$，其中$\mathfrak{A}=\ker\psi$. $S[x]/\mathfrak{A}[x]\cong\overline{S}[x]$.

14. 证 设$\mathfrak{A}$是$\mathbb{Z}/(p^n)$的任一非零理想，则$\exists[a]\in\mathfrak{A}$, $[a]\neq[0]$, 从而$\bar{a}\in(p^n)$. 因p是素数，故a与p^n的最大公因子为p^l. 因$a\,\overline{\in}\,(p^n)$，故$l\neq n$，即$0\leqslant l\leqslant n$. 由最大公因子性质，$\exists u,v\in\mathbb{Z}$，使得$p^l=ua+vp^n$. 因$\mathfrak{A}$是理想，故

$$[p^l]=[ua+vp^n]=[u][a]+[v][p^n]=[u][a]+[v][0]=[u][a]\in\mathfrak{A}.$$

又$[p^{n-1}]=[p^l][p^{n-l-1}]$，因$n>l$，故$n-l-1\geqslant0$. 再由$\mathfrak{A}$是理想，$[p^{n-1}]\in\mathfrak{A}$.

15. 证 $\forall a\in R$, $\phi: a\to[a]$是R到$R/\mathfrak{A}$的自然同态. 因$R/\mathfrak{A}$是幂零元环，故$\exists$正整数n，使得$[a]^n=[a^n]=[0]$，从而$a^n\in\mathfrak{A}$. 又$\mathfrak{A}$也是幂零元环，于是$\exists$正整数m，使得$(a^n)^m=0$，即$\exists$正整数nm，使得$a^{nm}=0$. 所以R是幂零元环.

16. 证 由第十二章,二,4,注 2)知,$\mathfrak{A}+\mathfrak{B}=\{a+b \mid a\in\mathfrak{A},b\in\mathfrak{B}\}$是$R$的理想.由第十二章,一,5,4),例4,因$\mathfrak{A}$是环$R$的理想,$\mathfrak{A}$是$R$的子环,故$\mathfrak{A}\cap\mathfrak{B}$是$\mathfrak{B}$的理想,且

$$(\mathfrak{A}+\mathfrak{B})/\mathfrak{A}\cong\mathfrak{B}/(\mathfrak{A}\cap\mathfrak{B}).$$

因$\mathfrak{B}\sim\mathfrak{B}/(\mathfrak{A}\cap\mathfrak{B})$,$\mathfrak{B}$是幂零元环,故由第十一章,三,1,17)知$\mathfrak{B}/(\mathfrak{A}\cap\mathfrak{B})$是幂零元环,于是$(\mathfrak{A}+\mathfrak{B})/\mathfrak{A}$是幂零元环.今$\mathfrak{A}$,$(\mathfrak{A}+\mathfrak{B})/a$都是幂零元环.由上面15题,$\mathfrak{A}+\mathfrak{B}$也是幂零元环.

17. 证 $\phi^{-1}(S)$是$\mathbb{Z}$的子环[①],由第十二章,三,2,注2),$\mathbb{Z}$的子环都是理想,从而$\phi^{-1}(S)$是$\mathbb{Z}$的理想.所以$\phi(\phi^{-1}(S))=S$是R的理想[②].

第十三章

1. 解 由第十三章,三,2知:设p是正整数,则

$$p\text{是素数}\Leftrightarrow(p)\text{是}\mathbb{Z}\text{的最大理想}.$$

而包含(30)的$\mathbb{Z}$的理想总共是:(1),(2),(3),(5),(6),(10),(15),(30).所以$\mathbb{Z}$的包含(30)的全部最大理想为(2),(3),(5).

2. 证 (反证法)设x不是Q上未定元,则∃不全为零的元$\frac{a_0}{b_0},\frac{a_1}{b_1},\cdots,\frac{a_n}{b_n}(\neq 0)\in Q$,使得

$$\frac{a_0}{b_0}+\frac{a_1}{b_1}x+\cdots+\frac{a_n}{b_n}x^n=0,$$

其中$a_i,b_i\in R,b_i\neq 0,i=0,1,2,\cdots,n$.用$b_0b_1\cdots b_n(\neq 0)$乘上式左右两边,得

$$a_0b_1b_2\cdots b_n+a_1b_0b_2b_3\cdots b_nx+\cdots+a_nb_0b_1\cdots b_{n-1}x^n=0.$$

因R无零因子,故$a_nb_0b_1\cdots b_{n-1}\neq 0$,从而$x$不是$R$上未定元,此与已知矛盾.所以$x$是$Q$上未定元.

注 设Q是整环R的商域,则Q上未定元x也是R上未定元.

3. 证一 设Q是R的一个商域.因$a,b\in R$,故$a,b\in Q$.

1) 若$b\neq 0$,则∃$b^{-1}\in Q$,因$a^m=b^m$,故

$$(ab^{-1})^m=a^m(b^{-1})^m=a^m(b^m)^{-1}=a^m(a^m)^{-1}=1.$$

同理$(ab^{-1})^n=1$.因m,n互素,故∃$u,v\in\mathbb{Z}$,使得$mu+nv=1$,从而

$$ab^{-1}=(ab^{-1})^{mu+nv}=((ab^{-1})^m)^u\cdot((ab^{-1})^n)^v=1.$$

所以$a=b$.

2) 若$b=0$,由$a^m=b^m$,R无零因子,有$a=0$,所以$a=b$.

证二 因m,n互素,故∃$u,v\in\mathbb{Z}$,使得$mu+nv=1$,从而

$$a=a^{mu+nv}=(a^m)^u\cdot(a^n)^v=(b^m)^u\cdot(b^n)^v=b^{mu+nv}=b.$$

第十四章

1. 证 (⇒) 因$\varepsilon+a$是I的单位,故∃$b\in I$,使得$(\varepsilon+a)b=\varepsilon b+ab=1$,即$ab=1-\varepsilon b$.因$a$是$I$的幂零元,故∃正整数$n$,使得$a^n=0$.因$I$是交换环,故

---

① ② 张禾瑞.近世代数基础.北京:高等教育出版社,1978.116.定理3.

$$\begin{aligned}0 &= a^n b^n = (ab)^n = (1-\varepsilon b)^n \\ &= 1 - C_n^1(\varepsilon b) + C_n^2(\varepsilon b)^2 - \cdots + (-1)^n C_n^n(\varepsilon b)^n \\ &= 1 - \varepsilon(C_n^1 b + C_n^2 \varepsilon b^2 - \cdots + (-1)^n \varepsilon^{n-1} b^n),\end{aligned}$$

从而$\exists\, c = C_n^1 b + C_n^2 \varepsilon b^2 - \cdots + (-1)^n \varepsilon^{n-1} b^n \in I$，使得$\varepsilon c = 1$. 所以$\varepsilon$是$I$的单位.

($\Leftarrow$) 因a是幂零元，故$\exists$正整数n，使得$a^n=0$. 因ε是I的单位，故$\exists\,\varepsilon^{-1}=\varepsilon_1\in I$，使得$\varepsilon\varepsilon_1=1$. 于是，由$I$是交换环，有

$$\begin{aligned}&(\varepsilon + a)(\varepsilon_1 - \varepsilon_1^2 a + \varepsilon_1^3 a^2 - \cdots + (-1)^{n-2}\varepsilon_1^{n-1}a^{n-2} + (-1)^{n-1}\varepsilon_1^n a^{n-1}) \\ &= \varepsilon\varepsilon_1 - \varepsilon\varepsilon_1^2 a + \varepsilon\varepsilon_1^3 a^2 - \cdots + (-1)^{n-2}\varepsilon\varepsilon_1^{n-1}a^{n-2} + (-1)^{n-1}\varepsilon\varepsilon_1^n a^{n-1} + \\ &\quad \varepsilon_1 a - \varepsilon_1^2 a^2 + \cdots + (-1)^{n-2}\varepsilon_1{}^{n-1}a^{n-1} + (-1)^{n-1}\varepsilon_1^n a^n = 1,\end{aligned}$$

其中$\varepsilon_1 - \varepsilon_1^2 a + \varepsilon_1^3 a^2 - \cdots + (-1)^{n-2}\varepsilon_1^{n-1}a^{n-2} + (-1)^{n-1}\varepsilon_1^n a^{n-1} \in I$. 所以$\varepsilon + a$是$I$的单位.

注 1) I是有单位元的交换环时，命题仍成立.

2) 参看第九章，四，12，5).

2. 证 显然相伴是I的元间的一个关系.

1) $\forall a\in I$，因$a=1a$，1是单位，故a是a的相伴元.

2) $\forall a,b\in I$，若a是b的相伴元，即$a\,|\,b$，$b\,|\,a$，从而b是a的相伴元.

3) $\forall a,b,c\in I$，若a是b的相伴元，b是c的相伴元，则$\exists$单元$\varepsilon,\varepsilon'\in I$，使得$a=\varepsilon b$，$b=\varepsilon' c$，从而$a=\varepsilon\varepsilon' c$，其中$\varepsilon\varepsilon'$是$I$的单位，于是$a$是$c$的相伴元.

所以相伴是I的元间的一个等价关系. 它就决定了I的一个分类. 取定$a\in I$，含a的相伴类是

$$\begin{aligned}[a] &= \left\{x\in I \,\middle|\, x,a\ 相伴\right\} = \left\{x\in I \,\middle|\, x = \varepsilon a, \varepsilon\ 是\ I\ 的单位\right\} \\ &= \left\{\varepsilon a \,\middle|\, \varepsilon\ 是\ I\ 的单位\right\}.\end{aligned}$$

注 1) 当ε_0是I的单位时，

$$[\varepsilon_0] = \left\{\varepsilon\varepsilon_0 \,\middle|\, \varepsilon\ 是\ I\ 的单位\right\} = \{I\ 的所有的单位\} = U.$$

所以I的所有的单位作成一个相伴类，是一个乘群. 而其余的相伴类$[a]=Ua$.

2) 取定$a(\neq 0)\in I$，$\phi:\varepsilon a\to\varepsilon$是$[a]$与$[\varepsilon_0]$间的一个一一映射，其中$\varepsilon$是$I$的单位. 事实上，$\forall\,\varepsilon a[a]$，$\exists$单位$\varepsilon=(\varepsilon\varepsilon_0^{-1})\varepsilon_0\in[\varepsilon_0]$，使得$\phi(\varepsilon a)=\varepsilon$. 且若$\varepsilon a=\varepsilon' a$，则因$a\neq 0$，故由消去律$\varepsilon=\varepsilon'$，即$\phi(\varepsilon a)=\phi(\varepsilon' a)$，所以$\phi$是映射. $\forall\,\varepsilon\varepsilon_0\in[\varepsilon_0]$，$\exists\,\varepsilon\varepsilon_0 a\in[a]$，使得$\phi(\varepsilon\varepsilon_0 a)=\varepsilon\varepsilon_0$，所以$\phi$是满射. $\forall\,\varepsilon a,\varepsilon' a\in[a]$，若$\phi(\varepsilon a)=\phi(\varepsilon' a)$，则$\varepsilon=\varepsilon'$，从而$\varepsilon a=\varepsilon' a$. 所以$\phi$是单射. 所以$\phi$是$[a]$与$[\varepsilon_0]$间的一个一一映射.

3) 在整数环$\mathbb{Z}$中，由相伴决定的相伴类是$[0]=\{0\}$，$[1]=\{1,-1\}$，…，$[2]=\{2,-2\}$，…，$[n]=\{n,-n\}$，…

4) 在实数域$\mathbb{R}$上的多项式环$\mathbb{R}[x]$中，相伴类$[f(x)]=\left\{rf(x)\,\middle|\,r\in\mathbb{R},r\neq 0\right\}$，即同一相伴类中的多项式系数成比例.

3. 解 例，

$$I = \left\{a_1x^{\alpha_1} + a_2x^{\alpha_2} + \cdots + a_nx^{\alpha_n} \,\middle|\, a_i \in 域\ F, \alpha_i\ 是非负有理数, n\ 是正整数\right\}$$

与普通多项式同样地定义I中的元的相等、相加与相乘. 可以证明I作成一个整环. 域F的单位元1就是I的单位元. 还可以证明

$$f(x)\text{ 是 }I\text{ 的单位}\Leftrightarrow f(x)\in F,\ f(x)\neq 0.$$

取 $x\in I$，于是 $x\neq 0$，$x\neq I$ 的单位. 则 x 在 I 里没有分解.

事实上，假定 x 在 I 里有分解：

$$x=f_1(x)f_2(x)\cdots f_r(x),$$

其中 $f_i(x)$是 I 的素元，$i=1,2,\cdots,r$. 因多项式 x 的常数项$=0$，故在 $f_i(x)$中必有常数项为 0 的多项式，不妨设 $f_1(x)$的常数项为 0，从而

$$f_1(x)=x^{\alpha}g(x),$$

其中 α 是 $f_1(x)$中指数最小的一项的指数. 因

$$x^{\alpha}=x^{\frac{\alpha}{2}}x^{\frac{\alpha}{2}}.$$

而 $x^{\frac{\alpha}{2}}$不是单位，故 $x^{\frac{\alpha}{2}}$是 x^{α} 的真因子，因此 $f_1(x)$有真因子 $x^{\frac{\alpha}{2}}$，从而 $f_1(x)$不是素元，发生矛盾. 所以 x 不能写成 I 的素元的乘积，即 x 在 I 里没有分解.

又例，

$$I=\left\{a_1 2^{\alpha_1}+a_2 2^{\alpha_2}+\cdots+a_n 2^{\alpha_n}\,\middle|\,a_i\in\mathbf{Z}\ ,n\text{ 是正整数}，\right.$$
$$\left.\alpha_i\text{ 是形如}\frac{m}{2^k}\text{ 的分数，这里 }m,k\text{ 是非负整数}\right\}$$

对于数的加法和乘法来说作成一个整环. 数 1 是 I 的单位元. 取 $2\in I$，$2\neq 0$，$2\neq I$ 的单位，则 2 在 I 里没有分解. 事实上，

$$2=2^{\frac{1}{2}}2^{\frac{1}{2}}=2^{\frac{1}{2}}2^{\frac{1}{4}}2^{\frac{1}{4}}=2^{\frac{1}{2}}2^{\frac{1}{4}}2^{\frac{1}{8}}2^{\frac{1}{8}}=\cdots$$

因$\left(2^{\frac{1}{2^k}}\right)^{-1}\overline{\in} I$，故 $2^{\frac{1}{2^k}}$不是 I 的单位，$k=0,1,2,\cdots$从而 2 有真因子 $2^{\frac{1}{2}}$，$2^{\frac{1}{2}}$有真因子 $2^{\frac{1}{4}}$，$2^{\frac{1}{4}}$有真因子 $2^{\frac{1}{8}}$，$\cdots$，$2^{\frac{1}{2^m}}$有真因子 $2^{\frac{1}{2^{m+1}}}$，$\cdots$这样无限下去. 于是 2 不能写成 I 的素元的乘积，即 2 在 I 里没有分解.

4. 证　1)　仿第十四章，二，3 和第十四章，三，5 可证①，②.

③　因 $7=(3+\sqrt{2})(3-\sqrt{2})$，$3\pm\sqrt{2}$是素元，故 7 有真因子 $3+\sqrt{2}$，所以 7 不是素元.

④　设 $\alpha(\neq\pm 1)$是 $\mathbf{Z}[\sqrt{2}]$的一个单位(这样的$\neq\pm 1$ 的单位是存在的，如 $1+\sqrt{2}$). 则

$$\alpha,\alpha^2,\alpha^3,\cdots,\alpha^n,\cdots$$

都是 $\mathbf{Z}[\sqrt{2}]$的单位. 若 $\alpha^n=\alpha^m$，则 $\alpha^{n-m}=1$. 但数 $\alpha\neq\pm 1$，从而 $n-m=0$，即 $n=m$. 因此，当 $n\neq m$ 时，$\alpha^n\neq\alpha^m$. 所以，在 $\mathbf{Z}[\sqrt{2}]$中有无限多个不同的单位.

2)　请读者自证①，②.

③　因 $6=2\cdot 3=(4+\sqrt{10})(4-\sqrt{10})$，其中 $2,3,4+\sqrt{10},4-\sqrt{10}$都是素元，$4+\sqrt{10},4-\sqrt{10}$都不是 2 的相伴元，也不是 3 的相伴元，故 6 的分解不唯一.

注　1)　$1+\sqrt{2},(1+\sqrt{2})^2=3+2\sqrt{2},(1+\sqrt{2})^3=7+5\sqrt{2},\cdots$都是 $\mathbf{Z}[\sqrt{2}]$的单位.

2)　实际上，$\mathbf{Z}[\sqrt{2}]$是唯一分解环(见第十五章，四，1)，而 $\mathbf{Z}[\sqrt{10}]$不是唯一分解环(因 6 的分解不唯一). 即使被开方数 r 是素数，$\mathbf{Z}[\sqrt{r}]$也未必是唯一分解环，如 $\mathbf{Z}[\sqrt{5}]$不是唯一分解环.

5. 证　易证 S_p 是环. $1=\frac{1}{1}(\in S_p)$是 S_p 的单位元. 因 S_p 是数环，故 S_p 是无零因子的

交换环. 即 S_p 是整环. 下面证明:设 $\frac{a}{b}\in S_p$,则

$$\frac{a}{b}\text{ 是 } S_p \text{ 的单位} \Leftrightarrow p\nmid a.$$

事实上,($\Rightarrow$) 因 $\frac{a}{b}$ 是 S_p 的单位,故 $\exists\ \frac{c}{d}\in S_p$,使得 $\frac{a}{b}\cdot\frac{c}{d}=1$,即 $ac=bd$. 因 $p\nmid b$, $p\nmid d$, p 是素数,故 $p\nmid bd$,从而 $p\nmid ac$,于是 $p\nmid a$ 且 $p\nmid c$.($\Leftarrow$) 若 $p\nmid a$,则 $\frac{b}{a}\in S_p$. 又 $\frac{a}{b}\cdot\frac{b}{a}=1$,从而 $\frac{a}{b}$ 有逆元 $\frac{b}{a}\in S_p$,于是 $\frac{a}{b}$ 是 S_p 的单位.

设 $\mathfrak{A}$ 是 S_p 的一个理想. 若 $\mathfrak{A}=\{0\}$,则显然 $\mathfrak{A}$ 是 S_p 的主理想. 若 $\mathfrak{A}\neq\{0\}$,

1) $\mathfrak{A}$ 中有 S_p 的单位 ε 时,$\mathfrak{A}=(\varepsilon)=S_p$ 是主理想.

2) $\mathfrak{A}$ 中无 S_p 的单位时,作集

$$A=\left\{n\,\middle|\,\frac{a}{b}\in\mathfrak{A},a=p^nc,p\nmid c\right\}.$$

则 A 是不空正整数集,从而 A 有最小正整数 n_0. 我们断言:$\mathfrak{A}=(p^{n_0})$. 事实上,$\forall\ \frac{a}{b}\in\mathfrak{A}$, $p\,|\,a$, $a=p^ma_1$, $p\nmid a_1$, $m\geqslant n_0$,于是 $\frac{a}{b}=\frac{p^ma_1}{b}=\frac{p^{m-n_0}a_1}{b}\cdot p^{n_0}\in(p^{n_0})$,即 $\mathfrak{A}\subset(p^{n_0})$;反之,$\forall\ \frac{u}{v}\cdot p^{n_0}\in(p^{n_0})$,其中 $\frac{u}{v}\in S_p$. 由 n_0 的取法知,$\exists\ \frac{a}{b}\in\mathfrak{A}$,使得 $a=p^{n_0}c$, $p\nmid c$. 又 $\frac{u}{v}\cdot p^{n_0}=\frac{bu}{cv}\cdot\frac{c}{b}\cdot p^{n_0}=\frac{bu}{cv}\cdot\frac{a}{b}$,其中 $p\nmid c$, $p\nmid v$,从而 $p\nmid cv$,于是 $\frac{bu}{cv}\in S_p$. 又 $\frac{a}{b}\in\mathfrak{A}$,由 $\mathfrak{A}$ 是 S_p 的理想,有 $\frac{u}{v}\cdot p^{n_0}\in\mathfrak{A}$,即 $(p^{n_0})\subset\mathfrak{A}$. 所以 $\mathfrak{A}=(p^{n_0})$ 是 S_p 的主理想.

综上,S_p 是主理想环.

注 1) 因 S_p 是主理想环,故 S_p 是唯一分解环.

2) $S_7=\left\{\frac{a}{b}\in\mathbb{Q}\,\middle|\,a,b\in\mathbb{Z},7\nmid b\right\}$ 是唯一分解环. 设 $\frac{a}{b}\in S_7$,则 $\frac{a}{b}$ 是 S_7 的单位 $\Leftrightarrow 7\nmid a$. 即 S_7 的所有单位作成的乘群 $U=\left\{\frac{a}{b}\in S_7\,\middle|\,7\nmid a\right\}$.

3) 参看第十三章,四,4,3).

6. 证 1) 因 a,b 互素,故由第十四章,二,7,注 1),$\exists\ s,t\in I$,使得 $sa+tb=1$,即 $sac+tbc=c$. 因 $a\,|\,bc$,故 $a\,|\,sac+tbc=c$.

2) 因 $a\,|\,c$,故 $\exists\ u\in I$,使得 $c=au$. 因 $b\,|\,c$,故 $b\,|\,au$. 又 a,b 互素,由 1),$b\,|\,u$,从而 $\exists\ v\in I$,使得 $u=bv$,因此 $c=au=abv$,所以 $ab\,|\,c$.

3) 因 I 是主理想环,故 p,a 有最大公因子,设其中一个为 d. 因 $d\,|\,p$, p 是素元,故 d 是单位或 $d=\varepsilon p$, ε 是单位. 若 d 是单位,则 p,a 互素;若 $d=\varepsilon p$, ε 是单位,由 $d\,|\,a$,有 $\varepsilon p\,|\,a$,于是 $p\,|\,a$.

4) 因 $p_1\,|\,a$,故 $\exists\ h\in I$,使得 $a=p_1h$. 又 $p_2\,|\,a$,从而 $p_2\,|\,p_1h$. 因 p_1,p_2 不相伴,p_1,p_2 是素元,故 $p_2\nmid p_1$. 因 I 是唯一分解环,故 $p_2\,|\,h$,于是 $\exists\ k\in I$,使得 $h=p_2k$,即 $a=p_1h=$

p_1p_2k，所以 $p_1p_2 \mid a$.

另一证法：因 p_1 是素元，故由 3)，$p_1 \mid p_2$ 或 p_1, p_2 互素. 若 $p_1 \mid p_2$，又 p_2 是素元，$p_1 \neq$ 单位，从而 p_1, p_2 相伴，此与题设矛盾. 所以 p_1, p_2 互素. 由 2)，$p_1p_2 \mid a$.

7. 证 1) $\forall x \in [b] = b + (a)$，$\exists y \in I$，使得 $x = b + ay$，即 $b = x - ay$. 因 a, b 互素，故 $\exists s, t \in I$，使得 $1 = as + bt = as + (x - ay)t = a(s - yt) + xt$，其中 $s - yt, t \in I$. 由第十四章，二，7，注 1)，a, t 互素.

2) 因 $1, a$ 互素，故 $[1] \in G$，即 $G \neq \varnothing$. $\forall [b], [c] \in G$，b, a 互素，c, a 互素，从而 $\exists h, k, u, v \in I$，使得 $1 = ah + bk$，$1 = au + cv$，于是

$$1 = (ah + bk)(au + cv) = a(hau + bku + hcv) + bc(kv).$$

因此 bc, a 互素. 即 $[b][c] = [bc] \in G$. 至于 $[b][c] = [bc]$ 的唯一性，可由 $I/(a)$ 是一个环，它对于乘法封闭得知. 所以 G 对于乘法封闭.

因 $G \subset I/(a)$，而环 $I/(a)$ 中乘法结合律成立，故 G 中乘法结合律也成立. 又 G 有单位元 $[1]$.

$\forall [b] \in G$，因 a, b 互素，故 $\exists s, t \in I$，使得 $1 = as + bt$，从而 a, t 互素，即 $[t] \in G$. 且 $[1] = [as + bt] = [a][s] + [b][t]$. 因 $[a] = [0]$，故 $[b][t] = [1]$. 即 $[b]$ 在 G 中有逆元 $[t]$. 所以 G 作成一个群.

注 1) 参看第十章，二，7，8.

2) 例，

$G_1 = \{[b] \in \mathbb{Z}/(7) \mid b \in \mathbb{Z}, b, 7 \text{互素}\} = \{[1], [2], [3], [4], [5], [6]\}$ 是一个群，含 $\phi(7) = 6$ 个元，其中 $\phi(n)$ 是尤拉 ϕ 函数.

$$G_2 = \{[b] \in \mathbb{Z}/(12) \mid b \in \mathbb{Z}, b, 12 \text{ 互素}\} = \{[1], [5], [7], [11]\}$$

是一个群，含 $\phi(12) = 4$ 个元.

8. 证 因 I 是主理想环，故 I 的理想都是主理想. 设 (b) 是 I 的理想且 $(b) \ni a$，则 b 必为 a 的因子. 若 a 是单位，则只有单位 ε 是 a 的因子，即只有一个理想 $(\varepsilon) = I \ni a$，若 $a \neq$ 单位，因 I 是主理想环，又 $a \neq 0$，故除相伴元外只有有限个素元是 a 的因子，从而 a 的因子除相伴元外也只有有限个. 所以只有有限个理想包含 a.

第十五章

1. 证 1) $\forall \alpha = a + b\sqrt{2} (\neq 0) \in \mathbb{Z}[\sqrt{2}]$，显然 $\phi: \alpha = a + b\sqrt{2} \to |\alpha\bar{\alpha}| = |a^2 - 2b^2|$ 是集 $\mathbb{Z}[\sqrt{2}] - \{0\}$ 到非负整数集的一个映射，其中 $\bar{\alpha} = a - b\sqrt{2}$.

2) 给定 $\alpha = a + b\sqrt{2} (\neq 0) \in \mathbb{Z}[\sqrt{2}]$，$\forall \beta = c + d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. 因 $\alpha \neq 0$，故 a, b 不全为 0，从而 $a^2 - 2b^2 \neq 0$，于是在实数域 $\mathbf{R}$ 中，

$$h = \frac{\beta}{\alpha} = \frac{c + d\sqrt{2}}{a + b\sqrt{2}} = \frac{(a - b\sqrt{2})(c + d\sqrt{2})}{a^2 - 2b^2} = \frac{ac - 2bd}{a^2 - 2b^2} + \frac{ad - bc}{a^2 - 2b^2}\sqrt{2} = h_1 + h_2\sqrt{2} \in \mathbf{R},$$

其中 $h_1 = \dfrac{ac - 2bd}{a^2 - 2b^2}$，$h_2 = \dfrac{ad - bc}{a^2 - 2b^2} \in \mathbf{Q}$. 因此有整数 q_1, q_2，使

$$|h_1-q_1|\leqslant\frac{1}{2},\quad |h_2-q_2|\leqslant\frac{1}{2}.$$

(见第十五章,二,3 的证明). 令 $q=q_1+q_2\sqrt{2}$,则 $q\in\mathbb{Z}[\sqrt{2}]$,于是

$$\beta=h\alpha=q\alpha+(h\alpha-q\alpha)=q\alpha+(h-q)\alpha=q\alpha+r,$$

其中 $r=(h-q)\alpha$. 因 $h\alpha=\beta\in\mathbb{Z}[\sqrt{2}]$, $q\alpha\in\mathbb{Z}[\sqrt{2}]$,故 $r\in\mathbb{Z}[\sqrt{2}]$. 从而 $r=0$ 或 $r\neq 0$.

我们有下面事实: $\forall s=s_1+s_2\sqrt{2},\ t=t_1+t_2\sqrt{2}\in\mathbb{Q}[\sqrt{2}]$, $\phi(s)=|s\bar{s}|=|s_1^2-2s_2^2|$, $\phi(t)=|t\bar{t}|=|t_1^2-2t_2^2|$,其中 $\bar{s}=s_1-s_2\sqrt{2}$, $\bar{t}=t_1-t_2\sqrt{2}$. 因此

$$\phi(st)=|(st)(\overline{st})|=|st\bar{s}\bar{t}|=|(s\ \bar{s})(t\ \bar{t})|=|s\bar{s}|\,|t\bar{t}|=\phi(s)\phi(t).$$

从而,当 $r\neq 0$ 时,

$$\phi(r)=\phi\big((h-q)\alpha\big)=\phi(h-q)\,\phi(\alpha)=\phi((h_1-q_1)+(h_2-q_2)\sqrt{2})\,\phi(\alpha)$$

$$=\Big|(h_1-q_1)^2-2(h_2-q_2)^2\Big|\,\phi(\alpha)\leqslant\left|\left(\frac{1}{2}\right)^2-2\left(\frac{1}{2}\right)^2\right|\phi(\alpha)=\frac{1}{4}\phi(\alpha)<\phi(\alpha).$$

所以 $\mathbb{Z}[\sqrt{2}]$是一个欧氏环.

注 1) 仿该题证法,可证明整环 $\mathbb{Z}[\sqrt{2}\,\mathrm{i}]=\{a+b\sqrt{2}\,\mathrm{i}\mid a,b\in\mathbb{Z}\}$ 也是一个欧氏环. 这里取

$$\phi:\alpha=a+b\sqrt{2}\,\mathrm{i}(\neq 0)\rightarrow x\,\bar{x}=a^2+2b^2,\text{其中 }\bar{\alpha}=a-b\sqrt{2}\,\mathrm{i}.$$

2) 整环 $\mathbb{Z}[\sqrt{3}\,\mathrm{i}]=\{a+b\sqrt{3}\,\mathrm{i}\mid a,b\in\mathbb{Z}\}$ 不是唯一分解环①,从而不是欧氏环. 但与之形式上很相像的整环 $\mathbb{Z}[\sqrt{2}\,\mathrm{i}]$却是欧氏环. 因此我们不能只从形式上看问题. 如果我们仿照证明 $\mathbb{Z}[\sqrt{2}\,\mathrm{i}]$是欧氏环的方法,规定, $\forall\alpha=a+b\sqrt{3}\,\mathrm{i}(\neq 0)\in\mathbb{Z}[\sqrt{3}\,\mathrm{i}]$, $\phi:\alpha=a+b\sqrt{3}\,\mathrm{i}\rightarrow\alpha\bar{\alpha}=a^2+3b^2$,其中 $\bar{\alpha}=a-b\sqrt{3}\,\mathrm{i}$. 类似地,我们有

$$\phi(r)=\phi\big((h-q)\alpha\big)=\phi(h-q)\,\phi(\alpha)=\phi((h_1-q_1)+(h_2-q_2)\sqrt{3}\mathrm{i})\,\phi(\alpha)$$

$$=\big[(h_1-q_1)^2+3(h_2-q_2)^2\big]\,\phi(\alpha)\leqslant\left[\left(\frac{1}{2}\right)^2+3\left(\frac{1}{2}\right)^2\right]\phi(\alpha)=\phi(\alpha).$$

即$\phi(r)\leqslant\phi(\alpha)$,因而得不出$\phi(r)<\phi(\alpha)$. 也就是说,利用证明 $\mathbb{Z}[\sqrt{2}\mathrm{i}]$是欧氏环的方法不能证明 $\mathbb{Z}[\sqrt{3}\,\mathrm{i}]$是欧氏环.

3) 类似可证 $I=\{a+b\lambda\mid a,b\in\mathbb{Z},\lambda\text{ 满足方程 }\lambda^2+\lambda+1=0\}$ 是一个欧氏环. 这里 λ 即为除 1 以外的三次单位根. 只需规定$\phi:\alpha=a+b\lambda(\neq 0)\rightarrow a^2+b^2-ab$.

2. 证 首先证明 I 是复数域$\mathbb{C}$的子环.

显然 I 是$\mathbb{C}$的不空子集. $\forall\alpha=a+b\sqrt{3}\,\mathrm{i},\beta=c+d\sqrt{3}\,\mathrm{i}\in I$,

$$\alpha-\beta=(a+b\sqrt{3}\,\mathrm{i})-(c+d\sqrt{3}\,\mathrm{i})=(a-c)+(b-d)\sqrt{3}\,\mathrm{i}.$$

当 a,b,c,d 都是整数时,显然 $\alpha-\beta\in I$.

当 a,b 与 c,d 两组数中,一组都是整数而另一组都是奇数的$\frac{1}{2}$时,显然 $a-c,b-d$ 都是

① 张禾瑞. 近世代数基础. 北京:高等教育出版社,1978. 129. 例.

奇数的$\frac{1}{2}$，从而 $\alpha-\beta\in I$.

当 a,b,c,d 都是奇数的$\frac{1}{2}$时，因奇数减奇数是偶数，故 $a-c,b-d$ 都是整数，从而 $\alpha-\beta\in I$.

所以无论在任何情况下，都有 $\alpha-\beta\in I$.

$$\alpha\beta=(a+b\sqrt{3}\,\mathrm{i})(c+d\sqrt{3}\,\mathrm{i})=(ac-3bd)+(bc+ad)\sqrt{3}\,\mathrm{i}.$$

当 a,b,c,d 都是整数时，显然 $\alpha\beta\in I$.

当 a,b 与 c,d 两组数中，一组都是整数而另一组都是奇数的$\frac{1}{2}$时，不妨设 $c=\frac{2k+1}{2}$，$d=\frac{2l+1}{2}$，其中 k,l 都是整数. 则

$$ac-3bd=\frac{2ak-6bl+a-3b}{2}.$$

$$bc+ad=\frac{2bk+2al+a+b}{2}.$$

$(ac-3bd)-(bc+ad)=ak-3bl-bk-al-2b$ 是整数. 因此 $ac-3bd,bc+ad$ 或都是整数或都是奇数的$\frac{1}{2}$，从而 $\alpha\beta\in I$.

当 a,b,c,d 都是奇数的$\frac{1}{2}$时，设 $a=\frac{2m+1}{2}$，$b=\frac{2n+1}{2}$，$c=\frac{2k+1}{2}$，$d=\frac{2l+1}{2}$，其中 m,n,k,l 都是整数. 则

$$ac-3bd=\frac{2mk+m+k-6nl-3l-3n-1}{2}.$$

$$bc+ad=\frac{2nk+n+k+2ml+l+m+1}{2}.$$

$(ac-3bd)-(bc+ad)=mk-3nl-nk-ml-2l-2n-1$ 是整数. 因此 $ac-3bd,bc+ad$ 或都是整数或都是奇数的$\frac{1}{2}$. 从而 $\alpha\beta\in I$.

所以，$\forall\,\alpha,\beta\in I$，有 $\alpha\beta\in I$.

综上，I 是 $\mathbb{C}$ 的子环. 又 I 有单位元 $1+0\sqrt{3}\mathrm{i}$. 因 $\mathbb{C}$ 无零因子且可换，故 I 也无零因子且可换. 所以 I 是整环.

1)　$\forall\,\alpha=a+b\sqrt{3}\,\mathrm{i}(\neq 0)\in I$，设$\phi:\alpha=a+b\sqrt{3}\,\mathrm{i}\to\alpha\bar{\alpha}=a^2+3b^2$，其中 $\bar{\alpha}=a-b\sqrt{3}\,\mathrm{i}$.

当 a,b 都是整数时，a^2+3b^2 是非负整数.

当 a,b 都是奇数的$\frac{1}{2}$时，设 $a=\frac{2m+1}{2}$，$b=\frac{2n+1}{2}$，其中 m,n 都是整数，则

$$a^2+3b^2=m^2+m+3n^2+3n+1$$

是非负整数.

所以ϕ是集 $I-\{0\}$到非负整数集的一个映射.

2)　给定 $\alpha=a+b\sqrt{3}\,\mathrm{i}(\neq 0)\in I$，$\forall\,\beta=c+d\sqrt{3}\,\mathrm{i}\in I$. 因 $\alpha\neq 0$，故 $\exists\,\alpha^{-1}\in\mathbb{C}$，使得 $h=\beta\alpha^{-1}=h_1+h_2\sqrt{3}\,\mathrm{i}\in\mathbb{C}$，其中 $h_1,h_2\in\mathbb{Q}$.

$\forall s=s_1+s_2\sqrt{3}\,\mathrm{i}, t=t_1+t_2\sqrt{3}\,\mathrm{i}\in\mathbf{Q}[\sqrt{3}\,\mathrm{i}], \phi(s)=s\bar{s}=s_1^2+3s_2^2, \phi(t)=t\bar{t}=t_1^2+3t_2^2$，其中 $\bar{s}=s_1-s_2\sqrt{3}\,\mathrm{i}, \bar{t}=t_1+t_2\sqrt{3}\,\mathrm{i}$. 因此

$$\phi(st)=st\,\overline{st}=st\bar{s}\,\bar{t}=(s\bar{s})(t\bar{t})=\phi(s)\phi(t).$$

可取出 q_1, q_2，它们或都是整数，或都是奇数的$\frac{1}{2}$，使

$$|h_1-q_1|\leqslant\frac{1}{4}\quad,\quad|h_2-q_2|\leqslant\frac{1}{2}.$$

事实上，根据有理数性质，可设 $h_1=h_1'+\frac{v_1}{u_1}$，$h_2=h_2'+\frac{v_2}{u_2}$，其中 h_1', h_2'是整数，$\frac{v_1}{u_1}, \frac{v_2}{u_2}$是零或正真分数.

① 若$\frac{v_1}{u_1}\leqslant\frac{1}{4}, \frac{v_2}{u_2}\leqslant\frac{1}{2}$，则取 $q_1=h_1', q_2=h_2'$可使

$$|h_1-q_1|=|h_1-h_1'|=\left|\frac{v_1}{u_1}\right|\leqslant\frac{1}{4}\ ,\ |h_2-q_2|=|h_2-h_2'|=\left|\frac{v_2}{u_2}\right|\leqslant\frac{1}{2}.$$

② 若$\frac{v_1}{u_1}\leqslant\frac{1}{4}$ ，$\frac{v_2}{u_2}>\frac{1}{2}$ ，有 $0<1-\frac{v_2}{u_2}<\frac{1}{2}$，则取 $q_1=h_1', q_2=h_2'+1$，可使

$$|h_1-q_1|\leqslant\frac{1}{4}\ ,\ |h_2-q_2|=|h_2-h_2'-1|=\left|\frac{v_2}{u_2}-1\right|<\frac{1}{2}.$$

③ 若$\frac{v_1}{u_1}>\frac{1}{4}$ ，$\frac{v_2}{u_2}>\frac{1}{4}$ ，有 $\left|\frac{1}{2}-\frac{v_1}{u_1}\right|<\frac{1}{4}, \left|\frac{1}{2}-\frac{v_2}{u_2}\right|<\frac{1}{4}$，则取 $q_1=\frac{2h_1'+1}{2}, q_2=\frac{2h_2'+1}{2}$，可使

$$|h_1-q_1|=\left|h_1-\frac{2h_1'+1}{2}\right|=\left|\frac{v_1}{u_1}-\frac{1}{2}\right|<\frac{1}{4},\ |h_2-q_2|<\frac{1}{4}<\frac{1}{2}.$$

④ 若$\frac{v_1}{u_1}>\frac{1}{4}, \frac{v_2}{u_2}\leqslant\frac{1}{4}$，有$\left|\frac{1}{2}-\frac{v_1}{u_1}\right|<\frac{1}{4}$，则取 $q_1=\frac{2h_1'+1}{2}, q_2=\frac{2h_2'+1}{2}$，可使

$$|h_1-q_1|<\frac{1}{4},\ |h_2-q_2|=\left|\frac{v_2}{u_2}-\frac{1}{2}\right|=\frac{1}{2}-\frac{v_2}{u_2}\leqslant\frac{1}{2}.$$

所以令 $q=q_1+q_2\sqrt{3}\,\mathrm{i}$，有 $q\in I$. 因此

$$\beta=h\alpha=q\alpha+(h\alpha-q\alpha)=q\alpha+(h-q)\alpha=q\alpha+r,$$

其中 $r=(h-q)\alpha$. 因 $h\alpha=\beta\in I, q\alpha\in I$，故 $r\in I$. 于是 $r=0$ 或

$$\phi(r)=\phi((h-q)\alpha)=\phi(h-q)\,\phi(\alpha)=\phi\big((h_1-q_1)+(h_2-q_2)\sqrt{3}\,\mathrm{i}\big)\,\phi(\alpha)$$
$$=[(h_1-q_1)^2+3(h_2-q_2)^2]\,\phi(\alpha)\leqslant\left[\left(\frac{1}{4}\right)^2+3\left(\frac{1}{2}\right)^2\right]\phi(\alpha)=\frac{13}{16}\phi(\alpha)<\phi(\alpha).$$

所以 I 是一个欧氏环.

3. 证 $\forall b\in I^*$，有$\phi(b)=\phi(b1)=\phi(b)\phi(1)$. 因 $0\overline{\in}\phi(I^*)$，故$\phi(b)\neq0$，可消去，得$\phi(1)=1$.

($\Rightarrow$) 若 a 是 I 的单位，则 $\exists a^{-1}\in I$，使得 $aa^{-1}=1$，从而$\phi(aa^{-1})=\phi(1)$，即$\phi(a)\phi(a^{-1})=1$. 因$\phi(a), \phi(a^{-1})$都是正整数，故$\phi(a)=1$.

($\Leftarrow$) 若$\phi(a)=1$，则 $a\neq0$. 因 I 是欧氏环，故对于 $a(\neq0), 1\in I$ 来说，$\exists q, r\in I$，使得 $1=qa+r$，其中 $r=0$ 或$\phi(r)<\phi(a)$. 若$\phi(r)<\phi(a)=1$，但$\phi(r)$是非负整数，则$\phi(r)=0$，此与 $0\overline{\in}\phi(I^*)$矛盾. 因而只能 $r=0$，即 $1=qa$，从而 a 是单位.

4. 解一 1) 将 $\mathbf{Z}_5$中的元$[a]$用 a 表示. 依第十五章，一，2 中命题的证明，在 $\mathbf{Z}_5[x]$中作带余除法：

$$
\begin{array}{r}
x-2 \\
x^2+3x+2 \enclose{longdiv}{x^3+x^2+x+1} \\
\underline{x^3+3x^2+2x} \\
-2x^2-x+1 \\
\underline{-2x^2-6x-4} \\
5x+5
\end{array}
$$

余式 $5x+5=0$，即 $f(x)=g(x)(x-2)+0$，从而 $g(x)\mid f(x)$.

2) 在 $\mathbb{Z}_7[x]$中，如同 1)作带余除法，得 $f(x)=g(x)(x-2)+(5x+5)$，余式 $5x+5\neq 0$，从而 $g(x)\nmid f(x)$.

解二 1) 因 $\mathbb{Z}_5$是域，故 $\mathbb{Z}_5[x]$是主理想环. $g(x)=(x+1)(x+[2])$，又 $f([-1])=[-1]+[1]+[-1]+[1]=[0]$，$f([-2])=[-8]+[4]+[-2]+[1]=[0]$，从而$[-1]$，$[-2]$是 $f(x)$的根，于是 $x+1\mid f(x)$，$x+[2]\mid f(x)$①. 因 $x+1$，$x+[2]$互素，故由第十四章，四，6，2)，$(x+1)(x+[2])\mid f(x)$. 即 $g(x)\mid f(x)$.

2) 在 $\mathbb{Z}_7[x]$中，$f([-2])=[-8]+[4]+[-2]+[1]=[-5]\neq[0]$，即$[-2]$不是 $f(x)$的根，因此 $x+[2]\nmid f(x)$②. 而 $g(x)=(x+1)(x+[2])$，于是 $g(x)\nmid f(x)$. 否则，若 $g(x)\mid f(x)$，又 $x+[2]\mid g(x)$，从而 $x+[2]\mid f(x)$，发生矛盾. 所以 $g(x)\nmid f(x)$.

5. 证 （反证法）若 $f_1(x),f_2(x),\cdots$中有无限个互不相伴的多项式. 设 $g_1(x)=f_1(x)$，$g_2(x),\cdots$是其中互不相伴的本原多项式序列，则 $g_{i+1}(x)\mid g_i(x)$，$i=1,2,\cdots$. 又设 $\deg g_1(x)=n$，这里 n 是非负整数. 下面证明 $\deg g_i(x)>\deg g_{i+1}(x)$，$i=1,2,\cdots$. 因 $g_{i+1}(x)\mid g_i(x)$，故 $\deg g_i(x)\geqslant\deg g_{i+1}(x)$，且 $\exists\, h_{i+1}(x)\in I[x]$，使得 $g_i(x)=h_{i+1}(x)g_{i+1}(x)$. 假如 $\deg g_i(x)=\deg g_{i+1}(x)$，由 $\deg g_i(x)=\deg h_{i+1}(x)+\deg g_{i+1}(x)$，有 $\deg h_{i+1}(x)=0$，从而 $h_{i+1}(x)=a_{i+1}\in I$，即 $g_i(x)=a_{i+1}g_{i+1}(x)$. 因 $g_i(x)$，$g_{i+1}(x)$都本原，故 a_{i+1}是单位. 于是 $g_i(x)$，$g_{i+1}(x)$相伴，矛盾. 所以 $\deg g_i(x)>\deg g_{i+1}(x)$，$i=1,2,\cdots$. 我们得到一个无限的非负整数序列：

$$n=\deg g_1(x)>\deg g_2(x)>\cdots\geqslant 0.$$

但 n 是有限非负整数，此为矛盾. 所以序列 $f_1(x),f_2(x),\cdots$中只含有有限个互不相伴的多项式.

6. 解 1) 因$\mathbb{Q}[x]$是主理想环，x^2+2 在$\mathbb{Q}$上不可约，故由第十四章，二，8，注 3)，$\mathbb{Q}[x]/(x^2+2)$是域. 因$[x]\neq[0]$，故$[x]$在$\mathbb{Q}[x]/(x^2+2)$中有逆元.

因 x，x^2+2 互素，故由第十四章，二，7，$\exists\, u(x),v(x)\in\mathbb{Q}[x]$，使得 $xu(x)+(x^2+2)v(x)=1$. 易见取$u(x)=-\dfrac{x}{2}$，$v(x)=\dfrac{1}{2}$，可使$x\left(-\dfrac{x}{2}\right)+(x^2+2)\left(\dfrac{1}{2}\right)=1$. 即$[x]\left[-\dfrac{x}{2}\right]+[x^2+2]\cdot\left[\dfrac{1}{2}\right]=[1]$. 因$[x^2+2]=[0]$，故$[x]\left[-\dfrac{x}{2}\right]=[1]$. 所以$\left[-\dfrac{x}{2}\right]=-\dfrac{x}{2}+(x^2+2)$是$[x]$的逆元.

2) $\mathbb{Z}_3[x]$是主理想环. 因 x^2+1 在 $\mathbb{Z}_3$中无根，故 x^2+1 在 $\mathbb{Z}_3$上不可约，于是

① ② 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 148. 定理 1.

$\mathbb{Z}_3[x]/(x^2+1)$是域. 因$[[2]x+[2]]$是$\mathbb{Z}_3[x]/(x^2+1)$中的非零元,故它有逆元.

因$[2]x+[2]$, x^2+1互素,故$\exists\,[2]x+1,-1\in\mathbb{Z}_3[x]$,使得$([2]x+[2])([2]x+1)+(x^2+1)(-1)=1$. 即$\big[[2]x+[2]\big]\big[[2]x+1\big]+[x^2+1][-1]=[1]$. 因$[x^2+1]=[0]$,故$\big[[2]x+[2]\big]\cdot\big[[2]x+1\big]=[1]$. 所以$\big[[2]x+1\big]=[2]+1+(x^2+1)$是$\big[[2]x+[2]\big]$的逆元.

7. 证 ($\Rightarrow$) 若$a_n+a_{n-1}x+\cdots+a_0x^n$不是不可约,又它$\neq 0$, $\neq$单位,则它可约,有真因子$b_m+\cdots+b_0x^m$,使$a_n+a_{n-1}x+\cdots+a_0x^n=(b_m+\cdots+b_0x^m)(c_k+\cdots+c_0x^k)$,于是$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0=(b_mx^m+\cdots+b_0)(c_kx^k+\cdots+c_0)$,其中$b_mx^m+\cdots+b_0$是$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$的真因子,此与已知条件矛盾. 所以$a_n+a_{n-1}x+\cdots+a_0x^n$不可约.

($\Leftarrow$) 仿必要性的证明可证.

8. 证 若$f(x)\neq g(x)$,设$h(x)=f(x)-g(x)$,则$h(x)\neq 0$. 由第十一章,四,1,10), $\deg h(x)\leqslant\max(\deg f(x),\deg g(x))<n$. 由已知, $h(a_i)=f(a_i)-g(a_i)=0$, $i=1,2,\cdots,n$,从而$h(x)$至少有n个不同的根,产生了矛盾①. 所以$f(x)=g(x)$.

9. 证 因在$Q[x]$中$q(x)\,\big|\,f(x)$,故$\exists\,h(x)\in Q[x]$,使得$f(x)=g(x)h(x)$,且$h(x)$的最高系数为1. 设$g(x)=\dfrac{b}{a}g_0(x)$, $h(x)=\dfrac{d}{c}h_0(x)$,其中$a(\neq 0)$, $c(\neq 0)$, $b,d\in I$, $g_0(x)$, $h_0(x)$在$I[x]$中本原. 于是$f(x)=\dfrac{bd}{ac}g_0(x),h_0(x)$. 由第十五章,一,5, $g_0(x)h_0(x)$本原. 因$f(x)$的最高系数为1,故$f(x)$在$I[x]$中本原. 由第十五章,一,6, $f(x)=\varepsilon g_0(x)h_0(x)$, ε是I的单位. 设$g_0(x)$, $h_0(x)$的最高系数分别为a_0,b_0,则$1=\varepsilon a_0b_0$,从而a_0是I的单位,即a_0的逆元$\in I$. 又由$g(x)=\dfrac{b}{a}g_0(x)$,有$1=\dfrac{b}{a}\cdot a_0$,因此a_0的逆元$\dfrac{b}{a}\in I$,所以$g(x)=\dfrac{b}{a}g_0(x)\in I[x]$.

10. 证一 因$\alpha(\in\mathbb{Q})$是$f(x)$的根,故$x-\alpha\,\big|\,f(x)$. 又$\mathbb{Z}$是唯一分解环, $\mathbb{Q}$是$\mathbb{Z}$的商域,由上面9题知$x-\alpha\in\mathbb{Z}[x]$,所以α是整数.

证二 设$\alpha=\dfrac{a}{b}\in\mathbb{Q}$, $a,b\in\mathbb{Z}$, a,b互素,则$x-\dfrac{a}{b}\,\Big|\,f(x)$,即$bx-a\,\big|\,bf(x)$,从而$\exists\,g(x)\in\mathbb{Z}[x]$,使得$bf(x)=(bx-a)g(x)$. 因$f(x)$的最高系数为1,故$f(x)$在$\mathbb{Z}[x]$中本原,且比较等式两端多项式的最高系数,知$g(x)$的最高系数为1,于是$g(x)$在$\mathbb{Z}[x]$中本原. 因$a,b$互素,故$bx-a$也在$\mathbb{Z}[x]$中本原. 由第十五章,一,5, $(bx-a)g(x)$在$\mathbb{Z}[x]$中本原. 所以b是$\mathbb{Z}$的单位,即$b=\pm 1$,因此$\alpha=\dfrac{a}{b}$是整数.

注 利用该命题可判断某些最高系数为1的整系数多项式的可约性.

例 证明x^2-28在$\mathbb{Q}$上不可约. 事实上,设a是任一整数,当$|a|\geqslant 6$时, $a^2-28>0$;当$|a|<6$时, $a^2-28<0$. 即任一整数a都不是x^2-28的根. 由该命题,若x^2-28在$\mathbb{Q}$中有根α,则α必为整数,因而x^2-28在$\mathbb{Q}$中没有根,所以x^2-28在$\mathbb{Q}$上不可约.

11. 证 ($\Rightarrow$) 因$f(x)$是$R[x]$的单位,故$\exists\,g(x)=b_0+b_1x+\cdots+b_mx^m\in R[x]$,使得$f(x)g(x)=1$. 从而有

---

① 张禾瑞. 近世代数基础. 北京:高等教育出版社, 1978. 149. 推论.

$$a_0b_0 = 1. \tag{0}$$
$$a_0b_1 + a_1b_0 = 0. \tag{1}$$
$$a_0b_2 + a_1b_1 + a_2b_0 = 0. \tag{2}$$
$$\vdots$$
$$\cdots + a_{n-2}b_2 + a_{n-1}b_1 + a_nb_0 = 0. \tag{n}$$
$$\vdots$$
$$a_{n-2}b_m + a_{n-1}b_{m-1} + a_nb_{m-2} = 0. \tag{m+n-2}$$
$$a_{n-1}b_m + a_nb_{m-1} = 0. \tag{m+n-1}$$
$$a_nb_m = 0. \tag{m+n}$$

由(0)，a_0，b_0 都是单位.$(m+n-1)$乘以 a_n，得 $a_{n-1}a_nb_m+a_n^2b_{m-1}=0$，由$(m+n)$，$a_n^2b_{m-1}=0$. $(m+n-2)$乘以 a_n^2，得 $a_{n-2}a_n^2b_m+a_{n-1}a_n^2b_{m-1}+a_n^3b_{m-2}=0$，由 $a_n^2b_{m-1}=0$ 和 $a_nb_m=0$，$a_n^3b_{m-2}=0$. 依此向上推，最后至(n)，总可得 $a_n^{m+1}b_0=0$. 因 b_0 是单位，故 $\exists b_0^{-1}\in R$. 用 b_0^{-1} 右乘之，得 $a_n^{m+1}=0$. 所以 a_n 是 R 的幂零元.

因 $a_n^{m+1}=0$，$R[x]$是交换环，故$(a_nx^n)^{m+1}=a_n^{m+1}(x^n)^{m+1}=0$，从而 a_nx^n 也是 $R[x]$的幂零元. 已知 $f(x)=(a_0+a_1x+\cdots+a_{n-1}x^{n-1})+a_nx^n$ 是 $R[x]$的单位. 由第十四章，四，1，注 1)，$f_1(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}$也是 $R[x]$的单位. 对于 $f_1(x)$，仿照对 $f(x)$的做法，依次做下去，同理可知 $a_{n-1},a_{n-2},\cdots,a_1$ 都是 R 的幂零元.

$(\Leftarrow)$　因 a_0 是 R 的单位，故 a_0 是 $R[x]$的单位. 因 a_1 是 R 的幂零元，故 a_1x 是 $R[x]$的幂零元. 又 $R[x]$是有单位元的交换环，从而由第十四章，四，1，注 1)，a_0+a_1x 是 $R[x]$的单位. 因 a_2 是 R 的幂零元，故 a_2x^2 是 $R[x]$的幂零元，再由第十四章，四，1，注 1)，$a_0+a_1x+a_2x^2$ 是 $R[x]$的单位. 依此类推，知 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$ 是 $R[x]$的单位.

例　$\mathbb{Z}_9$是有单位元的交换环，$\mathbb{Z}_9$有零因子. $[1]+[3]x\in\mathbb{Z}_9[x]$，其中$[1]$是 $\mathbb{Z}_9$的单位，$[3]$是 $\mathbb{Z}_9$的幂零元. 由该命题，$[1]+[3]x$ 是 $\mathbb{Z}_9[x]$的单位. 其逆元为$[1]+[6]x$.

12. 证　由第十一章，二，6，注 1)，四元数除环 $\bar{R}=\{a+bi+cj+dk \mid a,b,c,d\in\mathbb{R}\}$，其中 $i^2=j^2=k^2=-1$，$ij=-ji=k$，$jk=-kj=i$，$ki=-ik=j$. $\forall\alpha=a+bi+cj+dk\in\bar{R}$，

$$\alpha^2 = (a+bi+cj+dk)^2 = a^2-b^2-c^2-d^2+2abi+2acj+2adk.$$

因此，只要取 $\alpha\in\bar{R}$，适合 $a=0$，$b^2+c^2+d^2=1$，则 $\alpha^2=1$，即 α 是 x^2+1 的根. 而适合 $a=0$，$b^2+c^2+d^2=1$ 的 $\alpha=a+bi+cj+dk$ 在 $\bar{R}$ 中有无限多个，所以 x^2+1 在 $\bar{R}$ 中有无限多个根. 例如 $\pm i$，$\pm j$，$\pm k$都是 x^2+1 的根.

注　该命题说明，若环 R 不是整环，则 R 上 n 次多项式在 R 里未必至多有 n 个根. 甚至还可能有无限多个根.

再举一个例子：设 R 是一个无限加群. 定义，$\forall a,b\in R$，$ab=0$，则 R 是一个环. 显然 R 有零因子，不是整环. 设 $f(x)=a_1x+a_2x^2+\cdots+a_nx^n\in R[x]$，则 $\forall\alpha\in R$，有 $f(\alpha)=0$. 因此 R 中任一元都是 $f(x)$的根. 所以 $f(x)$ 在 R 里有无限多个根.

13. 证　若 $f(x)$在 I 中有真因子，则命题已成立. 设 $f(x)$在I 中无真因子. 若 $f(x)$在 $I[x]$中不是不可约. 因 $p\nmid a_n$，故 $a_n\neq0$，即 $f(x)\neq0$ 且 $f(x)\neq$单位. 从而 $f(x)$在 $I[x]$中可约. 于是 $f(x)$有真因子 $g(x)\in I[x]$，使得 $f(x)=g(x)h(x)$，其中 $h(x)(\in I[x])$也是 $f(x)$的真因子. 设 $g(x)=b_0+b_1x+\cdots+b_rx^r$，$h(x)=c_0+c_1x+\cdots+c_sx^s$. 因 $f(x)$在 I 中无真因子，故 $b_r\neq0$，$c_s\neq0$，

$0<r<n, 0<s<n$. 因 $p\mid a_0=b_0c_0$, I 是唯一分解环, p 是素元, 故 $p\mid b_0$ 或 $p\mid c_0$. 不妨设 $p\mid b_0$, 则, $p\nmid c_0$. 否则, 若 $p\mid c_0$, 从而 $p^2\mid b_0c_0=a_0$, 矛盾. 再者, $g(x)$ 的系数不能全被 p 整除. 否则 $p\mid g(x)h(x)=f(x)$, 即 $p\mid a_n$, 矛盾. 因此, $\exists b_k$ 是 $g(x)$ 的头一个不被 p 整除的系数, 即 $p\nmid b_k$, 但 $p\mid b_0, p\mid b_1, \cdots, p\mid b_{k-1}$. 因 $p\mid b_0$, 故 $k>0$. 又 $a_k=b_kc_0+b_{k-1}c_1+\cdots+b_0c_k$. 因 $k\leqslant r<n$, 故 $k<n$, 于是 $p\mid a_k$, 且 $p\mid b_0c_k, \cdots, p\mid b_{k-1}c_1$, 从而 $p\mid b_kc_0$. 已知 $p\nmid b_k$, $p\nmid c_0$, 此与 p 是唯一分解环 I 的素元矛盾. 所以, 在 $f(x)$ 于 I 中无真因子的情况下, $f(x)$ 在 $I[x]$ 中不可约.

注 1) 若 $f(x)$ 满足本题的条件, 则 $f(x)$ 可能在 I 中有真因子. 例, $\mathbb{Z}$ 是唯一分解环, $6+3x\in\mathbb{Z}[x]$, $\exists$ 素元 $2\in\mathbb{Z}$, 使得 $2\nmid 3, 2\mid 6, 2^2\nmid 6$, 而 $6+3x$ 在 $\mathbb{Z}$ 中有真因子 3.

2) 设 I 是唯一分解环, $f(x)\in I[x]$, 若 $f(x)$ 可约, 则 $f(x+1)$ 也可约. 事实上, 因 $f(x)$ 可约, 故 $f(x)$ 有真因子 $g(x)\in I[x]$, 使得 $f(x)=g(x)h(x)$, 其中 $h(x)\in I[x]$. 从而 $f(x+1)=g(x+1)h(x+1)$. 于是 $g(x+1)$ 是 $f(x+1)$ 的真因子. 显然 $f(x+1)\neq 0$, $f(x+1)\neq$ 单位. 所以 $f(x+1)$ 可约.

其逆否命题是: 设 I 是唯一分解环, $f(x)\in I[x]$, 若 $f(x+1)$ 不可约, 则 $f(x)$ 也不可约.

14. 证 因 $f(x)=\dfrac{x^p-1}{x-1}$, 故

$$f(x+1)=\frac{(x+1)^p-1}{x+1-1}=\frac{x^p+C_p^1x^{p-1}+C_p^2x^{p-2}+\cdots+C_p^{p-1}x}{x}$$
$$=x^{p-1}+C_p^1x^{p-2}+C_p^2x^{p-3}+\cdots+C_p^{p-1}.$$

因 $p\nmid 1, p\mid C_p^1, p\mid C_p^2, \cdots, p\mid C_p^{p-1}=p, p^2\nmid C_p^{p-1}=p$, 又 $f(x+1)$ 在 $\mathbb{Z}$ 中无真因子, 故由艾森斯坦因不可约性判别准则, $f(x+1)$ 在 $\mathbb{Z}[x]$ 中不可约, 从而 $f(x)$ 在 $\mathbb{Z}[x]$ 中也不可约.

15. 证

$$\phi: b_nx^n+b_{n-1}x^{n-1}+\cdots+b_0\to[b_n]x^n+[b_{n-1}]x^{n-1}+\cdots+[b_0].$$

显然是 $\mathbb{Z}[x]$ 到 $\mathbb{Z}_p[x]$ 的同态满射(见第十二章, 四, 13, 11)). 假设 $f(x)$ 在 $\mathbb{Z}$ 上不是不可约, 因 $f(x)\neq 0$, $\neq$ 单位, 故 $f(x)$ 在 $\mathbb{Z}$ 上可约. 又因 $f(x)$ 的最高系数为 1, 故 $f(x)$ 是 $\mathbb{Z}$ 上本原多项式. 于是 $f(x)=g(x)h(x)$, 其中 $0<\deg g(x)<\deg f(x)$, $0<\deg h(x)<\deg f(x)$. 因 ϕ 是同态, 故

$$\phi: f(x)=g(x)h(x)\to\bar{f}(x)=\bar{g}(x)\bar{h}(x).$$

因 $g(x), h(x)$ 的首项系数为 1, 故 $\bar{g}(x), \bar{h}(x)$ 的首项系数为 $[1]$, 从而 $0<\deg\bar{g}(x)<\deg\bar{f}(x)$, $0<\deg\bar{h}(x)<\deg\bar{f}(x)$, 于是 $\bar{g}(x), \bar{h}(x)$ 都不是 $\mathbb{Z}_p[x]$ 的单位. 由第十四章, 一, 6, $\bar{f}(x)$ 在 $\mathbb{Z}_p$ 上可约①, 此与已知矛盾. 所以 $f(x)$ 在 $\mathbb{Z}$ 上不可约.

注 将 $f(x)$ 的首项系数为 1 这一条件去掉后, 命题不成立.

例 设 p 是素数, $f(x)=px^2+(p+1)x+1=(px+1)(x+1)\in\mathbb{Z}[x]$, 则 $f(x)$ 在 $\mathbb{Z}$ 上可约. 但 $\bar{f}(x)=[p]x^2+[p+1]x+[1]=[1]x+[1]\in\mathbb{Z}_p[x]$, $\bar{f}$ 却在 $\mathbb{Z}_p$ 上不可约.

第十六章

1. 证 1) 由第十六章, 一, 1, 注 2) 的证明, E 的素子域是 E 的一切子域的交, 从

---

① 张禾瑞. 近世代数基础. 北京: 高等教育出版社, 1978. 127. 定理 3.

而$\Delta\subset F$.

2) 因$\sqrt{\pi}=(\sqrt[4]{\pi})^2,\pi=(\sqrt[4]{\pi})^4,\pi^{100}=(\sqrt[4]{\pi})^{400}\in\mathbf{Q}(\sqrt[4]{\pi})$,故$\mathbf{Q}(\sqrt{\pi},\sqrt[4]{\pi},\pi,\pi^{100})\subset\mathbf{Q}(\sqrt[4]{\pi})$.反之显然成立.故等式成立.

3) ($\Rightarrow$) 若某$a_i\neq0,0\leqslant i\leqslant n-1$,则$F$上多项式$f(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}\neq0$,而$f(\alpha)=0$.此与$\alpha$的次数为$n$矛盾.($\Leftarrow$) 显然成立.

4) 因$F[x],E[x]$都是主理想环[①],$F[x]$是$E[x]$的子环,故由第十四章,二,9知结论成立.

5) 假设$p(x)$在E上不是不可约,又$p(x)\neq0,\neq$单位,则$p(x)$在E上可约.因$\deg p(x)=3$,故$p(x)$在E中有根α,从而$2^m=(E:F)=(E:F(\alpha))(F(\alpha):F)=(E:F(\alpha))3$,于是$3\mid 2^m$,矛盾.

6) 因$\sqrt[7]{2}$在$\mathbf{Q}$上极小多项式是x^7-2,故$(\mathbf{Q}(\sqrt[7]{2}):\mathbf{Q})=$素数7.由第十六章,三,1,17)知$K=\mathbf{Q}(\sqrt[7]{2})$或$K=\mathbf{Q}$.

2. 证 假设$p(x)$在E中有根α,则因$p(x)$是F上最高系数为1的不可约多项式,故$p(x)$是α在F上极小多项式,从而$(F(\alpha):F)=\deg p(x)>1$.因$E$是$F$的有限扩域,故由第十六章,一,9,2)及第十六章,一,9,$(E:F)=(E:F(\alpha))(F(\alpha):F)$,于是$\deg p(x)\mid(E:F)$.此与$\deg p(x)$与$(E:F)$互素矛盾.所以$p(x)$在$E$中无根.

3. 证 因E是F的有限扩域,故由第十六章,二,9,可设$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$,$n$是一个正整数.对$n$作数学归纳法.

1) 当$n=1$时,有$E=F(\alpha_1)$.

2) 假定$n-1$时,命题成立,今看$n(>1)$时,已知$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$.$F(\alpha_1)$和$F(\alpha_2)$是包含$F$的两个$E$的子域,从而$F(\alpha_1)\supset F(\alpha_2)$或$F(\alpha_2)\supset F(\alpha_1)$,于是$E=F(\alpha_1,\alpha_3,\cdots,\alpha_n)$或$E=F(\alpha_2,\alpha_3,\cdots,\alpha_n)$.由归纳假定$E$是$F$的单扩域.

依归纳原理,命题成立.

4. 证 $E=F(\alpha)=F\left(\frac{\alpha^3}{\alpha+1}\right)(\alpha)=I(\alpha)$.下面证明$\alpha$是$I$上代数元.显然$\beta=\frac{\alpha^3}{\alpha+1}\in I\subset E$,$\alpha\in E$.在$E$中,$\beta(\alpha+1)=\alpha^3$,即$\alpha^3-\beta\alpha-\beta=0$.从而$\alpha$是$I$上非零多项式$x^3-\beta x-\beta$的根,因此$\alpha$是$I$上代数元,所以$E=I(\alpha)$是$I$的单代数扩域.

5. 证 因$E=F(\alpha)\supset I\supsetneqq F$,$\alpha$是$F$上超越元,故$\exists\beta=\frac{f(\alpha)}{g(\alpha)}\in I,\beta\overline{\in}F$,其中$g(\alpha)\neq0$,$f(x),g(x)\in F[x]$.从而$\alpha$是$I$上多项式$f(x)-\beta g(x)$的根.因$g(x)\neq0$(否则$g(\alpha)=0$,矛盾),故存在$g(x)$的$i$次项系数$b_i\neq0$.令$a_i$是$f(x)$的$i$次项系数,则$a_i-\beta b_i$是$f(x)-\beta g(x)$的$i$次项系数.于是$a_i-\beta b_i\neq0$.事实上,假设$a_i-\beta b_i=0$,则$\beta=\frac{a_i}{b_i}\in F$,此与$\beta\overline{\in}F$矛盾.所以$a_i-\beta b_i\neq0$,即$\alpha$是$I$上非零多项式$f(x)-\beta g(x)$的根,因此$\alpha$是$I$上代数元.

6. 证 取$K=\{E$中的F上的全体代数元$\}$.由第十六章,一,11,2)知K是F的代数扩域.且$\forall\alpha\in E,\alpha\overline{\in}K$,则$\alpha$是$K$上超越元.事实上,假设$\alpha$是$K$上代数元,由第十六章,二,

① 张禾瑞.近世代数基础.北京:高等教育出版社,1978.140.定理3;139.定理1.

6,α是F上代数元,又$\alpha\in E$,于是$\alpha\in K$,矛盾.所以α是K上超越元.

注 由证明知E中的K上代数元都在K中.

7. 证 假设$x^{p^n}-\beta$在F上不是不可约,又$x^{p^n}-\beta\neq 0$,$\neq$单位,则$x^{p^n}-\beta$在F上可约,可设$f(x)(\in F[x])$是$x^{p^n}-\beta$的一个真因子.因 ch $F=p$,故由第十章,三,4,2),$x^{p^n}-\beta=x^{p^n}-\alpha^{p^n}=(x-\alpha)^{p^n}$.今$f(x)$是$(x-\alpha)^{p^n}$的真因子,从而$f(x)=(x-\alpha)^{p^r}\in F[x]$,$0\leqslant r\leqslant n-1$.于是$\alpha^{p^r}\in F$.因此$\alpha^{p^{n-1}}=(\alpha^{p^r})^{p^{n-1-r}}\in F$,与已知矛盾.所以$x^{p^n}-\beta$在$F$上不可约.

8. 证 因E是F的代数扩域,$F\subset R\subset E$,故环R的元都是F上代数元.$\forall\alpha\in R,\alpha\neq 0$,有$F(\alpha)$是$F$的单代数扩域,于是$\alpha^{-1}\in F(\alpha)=F[\alpha]\subset R$.由$R\supset F$,$R$含非零元1,1是$R$的单位元.显然$R$对乘法可交换,从而$R$是$E$的子域.若$E$是域$F$的有限扩域,由第十六章,一,10,$E$是$F$的代数扩域,所以$E$的任一子环$R(\supset F)$是$E$的子域.

9. 证 设$(E:\mathbb{R})=n$,因$\mathbb{R}$上不可约多项式只有一次和二次的,故n只能是1,2.当$n=1$时,由第十六章,一,12,$E=\mathbb{R}$,当然$E\cong\mathbb{R}$.当$n=2$时,因 ch $\mathbb{R}\neq 2$,$(E:\mathbb{R})=2$,故由第十六章,二,8的证明中($\Rightarrow$) 2),$\exists\alpha\in E,\alpha\,\overline{\in}\,\mathbb{R}$,使得$E=\mathbb{R}(\alpha)$,且$\alpha$在$\mathbb{R}$上极小多项式是$x^2-s$,即$\alpha^2=s\in\mathbb{R}$,$\alpha=\sqrt{s}\,\overline{\in}\,\mathbb{R}$.因$\mathbb{R}$包含所有正实数的平方根,故$s$是负实数.于是$\alpha=\sqrt{s}=it$,其中$t\in\mathbb{R}$.所以$E=\mathbb{R}(\alpha)=\mathbb{R}(it)=\mathbb{R}(i)=\mathbb{C}$.当然$E\cong\mathbb{C}$.

10. 证一 显然,$E=F(\alpha)\supset F(\alpha^2)\supset F$.因$E$是$F$的有限扩域,故由第十六章,一,9知$(E:F)=(F(\alpha):F(\alpha^2))(F(\alpha^2):F)$.设$(F(\alpha):F(\alpha^2))=s$,$(F(\alpha^2):F)=t$,$(F(\alpha):F)=r$,即$r=st$.因$r$是奇数,故$s,t$都是奇数.假设$s\neq 1$,则$s\geqslant 3$,即$r=st\geqslant 3t$.$\alpha^2$在$F$上极小多项式$p(x)$的次数为$t$,设$p(x)=x^t+a_{t-1}x^{t-1}+\cdots+a_0$,从而$p(\alpha^2)=\alpha^{2t}+a_{t-1}\alpha^{2(t-1)}+\cdots+a_0=0$,即$\alpha$是$F$上非零多项式$g(x)=x^{2t}+a_{t-1}x^{2(t-1)}+\cdots+a_0$的根,于是$(F(\alpha):F)=r\leqslant 2t$,此与$r\geqslant 3t$矛盾.所以$s=1$.由第十六章,一,12,$E=F(\alpha)=F(\alpha^2)$.

证二 由证一,$(F(\alpha):F)=(F(\alpha):F(\alpha^2))(F(\alpha^2):F)$.设$(F(\alpha):F)=2k+1$,其中$k$是非负整数,则由第十六章,一,5,$\forall\beta\in F(\alpha)$,$\beta=\sum_0^{2k}a_i\alpha^i=[a_0+a_2\alpha^2+\cdots+a_{2k}(\alpha^2)^k]+[a_1+a_3\alpha^2+\cdots+a_{2k-1}(\alpha^2)^{k-1}]\alpha$,其中$a_i\in F$,即$F(\alpha)$中每个元$\beta$可表为$1,\alpha$在$F(\alpha^2)$上的线性组合,从而$F(\alpha)$在$F(\alpha^2)$上的维数最多是2,于是$(F(\alpha):F(\alpha^2))=1$或$(F(\alpha):F(\alpha^2))=2$.但$(F(\alpha):F(\alpha^2))\mid(F(\alpha):F)=2k+1$,因此$(F(\alpha):F(\alpha^2))\neq 2$,所以$(F(\alpha):F(\alpha^2))=1$,即$E=F(\alpha)=F(\alpha^2)$.

证三 显然$F(\alpha^2)\subset F(\alpha)$;反之,设$(F(\alpha):F)=2k+1$,其中$k$是非负整数.设$x^{2k+1}+a_{2k}x^{2k}+\cdots+a_0$是$\alpha$在$F$上极小多项式,则$\alpha(\alpha^{2k}+a_{2k-1}\alpha^{2(k-1)}+\cdots+a_1)+(a_{2k}\alpha^{2k}+a_{2k-2}\alpha^{2(k-1)}+\cdots+a_0)=0$,其中$\beta=\alpha^{2k}+a_{2k-1}\alpha^{2(k-1)}+\cdots+a_1(\in F(\alpha^2))\neq 0$,否则$\alpha$是$F$上非零多项式$x^{2k}+a_{2k-1}x^{2(k-1)}+\cdots+a_1$的根,于是$(F(\alpha):F)=2k+1<2k$,矛盾.因此$\exists\beta^{-1}\in F(\alpha^2)$,使得$\alpha=-(a_{2k}\alpha^{2k}+a_{2k-2}\alpha^{2(k-1)}+\cdots+a_0)\beta^{-1}\in F(\alpha^2)$,从而$F(\alpha)\subset F(\alpha^2)$.所以$E=F(\alpha)=F(\alpha^2)$.

证四 显然$F(\alpha^2)\subset F(\alpha)$;反之,假设$\alpha\,\overline{\in}\,F(\alpha^2)$,则$\alpha$在$F(\alpha^2)$上极小多项式为$x^2-\alpha^2$,即$(F(\alpha^2)(\alpha):F(\alpha^2))=2$.但$F(\alpha^2)(\alpha)=F(\alpha)$,从而$(F(\alpha):F(\alpha^2))=2$.又$(F(\alpha):F)=(F(\alpha):F(\alpha^2))(F(\alpha^2):F)$,此与$(F(\alpha):F)$是奇数矛盾.所以$\alpha\in F(\alpha^2)$,即$F(\alpha)\subset F(\alpha^2)$.于是$E=F(\alpha)=F(\alpha^2)$.

第十七章

1. 证 假设 E 不是代数闭域，则 E 有真代数扩域 K，从而 $\exists \alpha \in K, \alpha \overline{\in} E$. 因 α 是 E 上代数元，故由第十六章，二，6，α 是 F 上代数元. 于是 α 是 F 上多项式 $f(x)(\overline{\in} F)$ 的一个根. 根据已知，$\alpha \in E$，此与 $\alpha \overline{\in} E$ 矛盾. 所以 E 是代数闭域.

2. 证 设 E 是 $f(x)$ 在 I 上的分裂域，$\alpha(\in E)$ 是 $f(x)$ 的根. 因 I 是 F 的有限扩域，故由第十六章，一，10，I 是 F 的代数扩域. 又 α 是 I 上代数元，故由第十六章，二，6，α 是 F 上代数元. 从而存在 α 在 F 上极小多项式 $g(x)$. 因在 $E[x]$ 中，$f(x)$，$g(x)$ 有公因子 $x-\alpha$，故在 $E[x]$ 中，$f(x)$，$g(x)$ 不互素. 因 $I[x]$，$E[x]$ 都是主理想环，$I[x]$ 是 $E[x]$ 的子环，故由第十四章，二，9，在 $I[x]$ 中，$f(x)$，$g(x)$ 也不互素. 而 $f(x)$ 在 I 上不可约，且 $I[x]$ 是主理想环，所以由第十四章，四，6，3)，在 $I[x]$ 中，$f(x) \mid g(x)$.

3. 证一 对 n 作数学归纳法.

1) $n=1$ 时，$f(x)=x-\alpha$，$\alpha \in F$，于是 $E=F(\alpha)=F$，所以由第十六章，一，12，$(E:F)=(F:F)=1 \leqslant 1!$.

2) 假定对于 F 上 $n-1(n \geqslant 2)$ 次多项式来说，命题成立. 今看 n 时. 设 $f(x) \in F[x]$，$\deg f(x)=n$，$f(x)$ 在 F 上的分裂域是 E，则 $f(x)=a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$，其中 $a_n \in F, \alpha_i \in E$. 由第十六章，一，6，注 3)，存在 α_1 在 F 上极小多项式 $g(x)$. 因 $f(\alpha_1)=0$，故由第十六章，一，6，2)，(1)，$g(x) \mid f(x)$. 于是 $(F(\alpha_1):F)=\deg g(x) \leqslant n$. 令 $h(x)=(x-\alpha_2)\cdots(x-\alpha_n)$，则 $f(x)=a_n(x-\alpha_1)h(x)$. 从而 $\deg h(x)=n-1$. 因 $f(x) \in F[x] \subset F(\alpha_1)[x]$，$x-\alpha_1 \in F(\alpha_1)[x]$，故 $h(x) \in F(\alpha_1)[x]$. 因 $h(x)$ 在 $F(\alpha_1)$ 上的分裂域为 $F(\alpha_1)(\alpha_2,\cdots,\alpha_n)=F(\alpha_1,\alpha_2,\cdots,\alpha_n)=E$，从而由归纳假定，$(E:F(\alpha_1)) \leqslant (n-1)!$. 所以

$$(E:F)=(E:F(\alpha_1))(F(\alpha_1):F) \leqslant (n-1)! \cdot n = n!.$$

证二 对 n 作数学归纳法.

1) $n=1$ 时，命题显然成立.

2) 假定对于 F 上 $n-1(n \geqslant 2)$ 次多项式来说，命题成立. 今看 n 时，设 $f(x)$ 是 F 上 n 次多项式，E 是 $f(x)$ 在 F 上的分裂域. 因 $F[x]$ 是唯一分解环，故 $f(x)$ 在 F 上有最高系数为 1 的不可约多项式 $g(x)$，从而 $\deg g(x) \leqslant n$. 由第十六章，二，4，存在 F 的单代数扩域 $F(\alpha_1)$，其中 α_1 在 F 上极小多项式是 $g(x)$. 于是 $(F(\alpha_1):F) \leqslant n$. 且 $f(x)=a_n(x-\alpha_1)h(x)$，其中 $h(x) \in F(\alpha_1)[x]$，$\deg h(x)=n-1$，同时 $h(x)$ 在 $F(\alpha_1)$ 上的分裂域是 E. 由归纳假定，$(E:F(\alpha_1)) \leqslant (n-1)!$. 所以 $(E:F) \leqslant n!$.

4. 证 1) 由第十七章，一，6，E 是 $x^q-x=x(x^{q-1}-1)$ 在 E 的素子域上的分裂域，从而 E 中 $q-1$ 个非零元 $\alpha_1,\alpha_2,\cdots,\alpha_{q-1}$ 是 $x^{q-1}-1$ 的 $q-1$ 个不同的根，即 $x^{q-1}-1=(x-\alpha_1)\cdot(x-\alpha_2)\cdots(x-\alpha_{q-1})$. 比较系数，得 $-1=(-1)^{q-1}\alpha_1\alpha_2\cdots\alpha_{q-1}$，即 $\alpha_1\alpha_2\cdots\alpha_{q-1}=(-1)^q=(-1)^{p^n}$. 当 $p=2$ 时，$(-1)^{p^n}=1=-1$；当 p 是奇素数时 $(-1)^{p^n}=-1$. 所以 $\alpha_1\alpha_2\cdots\alpha_{q-1}=-1$.

2) 因 $\mathbf{Z}_p=\{[0],[1],[2],\cdots,[p-1]\}$ 是含素数 p 个元的有限域. 由本题 1)，$[1][2]\cdots[p-1]=[-1]$，即 $[(p-1)!]=[-1]$，所以 $(p-1)! \equiv -1(p)$.

5. 证 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$，$a_i \in \Delta$. 由第十七章，一，6 中命题的证明，$\Delta$

中的元都是 x^p-x 的根，从而 $a_i^p=a_i, i=0,1,2,\cdots,n$. 于是由第十章，三，4，3)，

$$\begin{aligned} f(\alpha^p) &= a_n(\alpha^p)^n + a_{n-1}(\alpha^p)^{n-1} + \cdots + a_0 \\ &= a_n^p(\alpha^n)^p + a_{n-1}^p(\alpha^{n-1})^p + \cdots + a_0^p \\ &= (a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0)^p = (f(\alpha))^p = 0. \end{aligned}$$

所以 α^p 是 $f(x)$的一个根. 同理，

$$\begin{aligned} f(\alpha^{p^2}) &= a_n(\alpha^{p^2})^n + a_{n-1}(\alpha^{p^2})^{n-1} + \cdots + a_0 \\ &= a_n^p(\alpha^{pn})^p + a_{n-1}^p(\alpha^{p(n-1)})^p + \cdots + a_0^p \\ &= (a_n(\alpha^p)^n + a_{n-1}(\alpha^p)^{n-1} + \cdots + a_0)^p = (f(\alpha^p))^p = 0. \end{aligned}$$

所以 α^{p^2} 是 $f(x)$的一个根. 同理，$f(\alpha^{p^3})=(f(\alpha^{p^2}))^p=0,\cdots,f(\alpha^{p^n})=(f(\alpha^{p^{n-1}}))^p=0$. 所以 $\alpha^{p^3},\cdots,\alpha^{p^n}$ 都是 $f(x)$的根.

因 $f(x)$是 Δ 上 n 次不可约多项式，故$(\Delta(\alpha):\Delta)=n$，又 $\mathrm{ch}\Delta(\alpha)=p$，于是 $\Delta(\alpha)$是含 p^n 个元的有限域[①]. 由第十七章，一，6，$\Delta(\alpha)$是 $x^{p^n}-x$ 在 Δ 上的分裂域. 今 $\alpha\in\Delta(\alpha)$，由第十七章，一，7 中命题的证明，$\alpha^{p^n}-\alpha=0$，即 $\alpha^{p^n}=\alpha$.

6. 证 ($\Rightarrow$) 因 G 是循环群，故 $\exists g\in G$，使得 $G=(g)$. 又 G 是有限循环群，从而可设 $|G|=|g|=n$，则 n 是使 $g^n=e$ 成立的最小正整数. $\forall g^k\in G$，k 是整数，有$(g^k)^n=e$. 所以$|G|=n$ 是使$a^n=e(\forall a\in G)$成立的最小正整数.

($\Leftarrow$) 因 G 是有限交换群，故由第四章，二，6，$\exists n$ 是 G 的所有元的阶中最大者. 设 $g(\in G)$的阶是 n，由第十七章，一，8 知，$\forall a\in G$，$|a|\,\big|\,n$，从而 $a^n=e$. 于是 $n=|g|$是使 G 中每个元 a 满足条件 $a^n=e$ 的最小正整数. 由已知条件，G 的阶$|G|$是使 $a^n=e(\forall a\in G)$成立的最小正整数 n，所以$(g)=G$，G 是由 g 生成的循环群.

7. 解 1) $\beta=\sqrt{2}$在$\mathbf{Q}$上极小多项式是 x^2-2，其根为 $\beta=\beta_1=\sqrt{2},\beta_2=-\sqrt{2}$. $\gamma=\mathrm{i}$ 在$\mathbf{Q}$上极小多项式是 x^2+1，其根为 $\gamma=\gamma_1=\mathrm{i},\gamma_2=-\mathrm{i}$. $c\neq\dfrac{\beta_1-\beta_1}{\gamma_1-\gamma_2}=0$，$c\neq\dfrac{\beta_2-\beta_1}{\gamma_1-\gamma_2}=\dfrac{-\sqrt{2}-\sqrt{2}}{\mathrm{i}-(-\mathrm{i})}=\dfrac{-\sqrt{2}}{\mathrm{i}}$. 取 c 为除 0 外的任意一个有理数都是可以的. 今取 $c=1$，此时 $\theta=\beta+c\gamma=\sqrt{2}+\mathrm{i}$. 所以 $\mathbf{Q}(\sqrt{2},\mathrm{i})=\mathbf{Q}(\sqrt{2}+\mathrm{i})$.

2) 与 1)同理有$\mathbf{Q}(\sqrt{3},\sqrt[3]{2})=\mathbf{Q}(\sqrt{3}+\sqrt[3]{2})$.

3) 由第十七章，三，3，5)知，$\beta=\sqrt[5]{2}$在$\mathbf{Q}$上极小多项式是 x^5-2，其根为 $\beta=\beta_1=\sqrt[5]{2},\beta_2=\omega\sqrt[5]{2},\beta_3=\omega^2\sqrt[5]{2},\beta_4=\omega^3\sqrt[5]{2},\beta_5=\omega^4\sqrt[5]{2}$. ω 在$\mathbf{Q}$上极小多项式是 $x^4+x^3+x^2+x+1$，其根为 $\gamma=\gamma_1=\omega,\gamma_2=\omega^2,\gamma_3=\omega^3,\gamma_4=\omega^4$. 取 $c\neq\dfrac{\beta_i-\beta_1}{\gamma_1-\gamma_j}$，$j\neq1$，$j=2,3,4$，$i=1,2,3,4,5$. 今取 $c=1$，则 $\theta=\beta+c\gamma=\sqrt[5]{2}+\omega$. 所以$\mathbf{Q}(\sqrt[5]{2},\omega)=\mathbf{Q}(\sqrt[5]{2}+\omega)$.

4) 与 1)同理有$\mathbf{Q}(\sqrt{2}\,\mathrm{i},\omega)=\mathbf{Q}(\sqrt{2}\,\mathrm{i}+\omega)=\mathbf{Q}\left(\dfrac{-1+(2\sqrt{2}+\sqrt{3})\mathrm{i}}{2}\right)$.

5) $\beta=\omega$ 在$\mathbf{Q}$上极小多项式是 x^2+x+1，其根为 $\beta=\beta_1=\omega,\beta_2=\omega^2$. $\gamma=\gamma_1=2\mathrm{i}$ 在$\mathbf{Q}$上

① 张禾瑞. 近世代数基础. 北京：高等教育出版社，1978. 171. 定理 1.

极小多项式是 x^2+4，其根为 $\gamma=\gamma_1=2i,\gamma_2=-2i$. 取 $c\neq\frac{\beta_i-\beta_1}{\gamma_1-\gamma_j},j\neq1,j=2,i=1,2$. 今取 $c=\frac{1}{2}$，则 $\theta=\beta+c\gamma=\omega+i$. 所以 $\mathbb{Q}(\omega,2i)=\mathbb{Q}(\omega+i)$.

8. 解 1) 因 $\sqrt{2}+i\overline{\in}\mathbb{R}$，故 $\sqrt{2}+i$ 在 $\mathbb{R}$ 上没有一次极小多项式. 又因

$$[x-(\sqrt{2}+i)][x-(\sqrt{2}-i)]=x^2-2\sqrt{2}x+3\in\mathbb{R}[x].$$

故 $x^2-2\sqrt{2}x+3$ 是 $\sqrt{2}+i$ 在 $\mathbb{R}$ 上极小多项式.

2) 设 $\alpha=\sqrt{2}+i$，则 $\alpha^2=1+2\sqrt{2}i,(\alpha^2-1)^2=(2\sqrt{2}i)^2$，从而 $\alpha^4-2\alpha^2+9=0$. 因此 α 是 $\mathbb{Q}$ 上多项式 $p(x)=x^4-2x^2+9$ 的根. 因 i 在 $\mathbb{Q}(\sqrt{2})$ 上极小多项式是 x^2+1，$\sqrt{2}$ 在 $\mathbb{Q}$ 上极小多项式是 x^2-2，故

$$(\mathbb{Q}(\sqrt{2}+i):\mathbb{Q})=(\mathbb{Q}(\sqrt{2})(i):\mathbb{Q}(\sqrt{2}))(\mathbb{Q}(\sqrt{2}):\mathbb{Q})=2\cdot2=4.$$

所以 $p(x)=x^4-2x^2+9$ 是 $\sqrt{2}+i$ 在 $\mathbb{Q}$ 上极小多项式.

3) $1,\sqrt{2}+i,(\sqrt{2}+i)^2,(\sqrt{2}+i)^3$ 是 $\mathbb{Q}(\sqrt{2}+i)$ 在 $\mathbb{Q}$ 上的一个基.

另一求法，由第十六章，一，9 中命题的证明知，$\mathbb{Q}(\sqrt{2},i)$ 在 $\mathbb{Q}(\sqrt{2})$ 上的一个基 $1,i$ 与 $\mathbb{Q}(\sqrt{2})$ 在 $\mathbb{Q}$ 上的一个基 $1,\sqrt{2}$ 分别相乘即得 $\mathbb{Q}(\sqrt{2},i)$ 在 $\mathbb{Q}$ 上的一个基. 因此，$1,\sqrt{2},i,\sqrt{2}i$ 是 $\mathbb{Q}(\sqrt{2},i)$ 在 $\mathbb{Q}$ 上的一个基.

4) 因 $\sqrt{2}+i\in\mathbb{Q}(\sqrt{2},i)$，故 $\mathbb{Q}(\sqrt{2}+i)\subset\mathbb{Q}(\sqrt{2},i)$. 由第十六章，一，9，

$(\mathbb{Q}(\sqrt{2},i):\mathbb{Q})=(\mathbb{Q}(\sqrt{2},i):\mathbb{Q}(\sqrt{2}+i))(\mathbb{Q}(\sqrt{2}+i):\mathbb{Q})=(\mathbb{Q}(\sqrt{2},i):\mathbb{Q}(\sqrt{2}+i))\cdot4$. 又 $(\mathbb{Q}(\sqrt{2},i):\mathbb{Q})=4$，从而 $(\mathbb{Q}(\sqrt{2},i):\mathbb{Q}(\sqrt{2}+i))=1$. 由第十六章，一，12，$\mathbb{Q}(\sqrt{2},i)=\mathbb{Q}(\sqrt{2}+i)$.

另一证法，令 $\alpha=\sqrt{2}+i$，则 $(\sqrt{2}-\alpha)^2=(-i)^2$，即 $2+\alpha^2-2\sqrt{2}\alpha=-1$，于是 $\sqrt{2}=\frac{3+\alpha^2}{2\alpha}\in\mathbb{Q}(\alpha)$. 又 $(i-\alpha)^2=(-\sqrt{2})^2$，即 $-1+\alpha^2-2\alpha i=2$，于是 $i=\frac{3-\alpha^2}{-2\alpha}\in\mathbb{Q}(\alpha)$. 所以 $\mathbb{Q}(\sqrt{2},i)\subset\mathbb{Q}(\alpha)$；反之，显然成立. 所以 $\mathbb{Q}(\sqrt{2},i)=\mathbb{Q}(\sqrt{2}+i)$.

另一证法，因 $(\sqrt{2}+i)^{-1}=\frac{1}{\sqrt{2}+i}=\frac{\sqrt{2}-i}{(\sqrt{2}+i)(\sqrt{2}-i)}=\frac{1}{3}(\sqrt{2}-i)\in\mathbb{Q}(\sqrt{2}+i)$，故 $\sqrt{2}-i=3\cdot\frac{1}{3}(\sqrt{2}-i)\in\mathbb{Q}(\sqrt{2}+i)$. 从而 $i=\frac{1}{2}[(\sqrt{2}+i)-(\sqrt{2}-i)]\in\mathbb{Q}(\sqrt{2}+i)$，$\sqrt{2}=\frac{1}{2}[(\sqrt{2}+i)+(\sqrt{2}-i)]\in\mathbb{Q}(\sqrt{2}+i)$. 于是 $\mathbb{Q}(\sqrt{2},i)\subset\mathbb{Q}(\sqrt{2}+i)$；反之，显然成立. 所以 $\mathbb{Q}(\sqrt{2},i)=\mathbb{Q}(\sqrt{2}+i)$.

9. 证 若 $d(x)=(f(x),f'(x))=1$，则结论显然成立. 若 $d(x)\neq1$，即 $f(x)$，$f'(x)$ 不互素，则由第十七章，一，11，1)知，$f(x)$ 在 F 上的分裂域 E 中有重根. 设

$$f(x)=(x-\alpha_1)^{s_1}(x-\alpha_2)^{s_2}\cdots(x-\alpha_t)^{s_t},$$

其中 $\alpha_i\in E,s_i\geqslant1,\alpha_i\neq\alpha_j(i\neq j)$. 因 $\mathrm{ch}\,F=\infty$，故

$$f'(x)=s_1(x-\alpha_1)^{s_1-1}(x-\alpha_2)^{s_2}\cdots(x-\alpha_t)^{s_t}+\cdots$$
$$+s_t(x-\alpha_1)^{s_1}(x-\alpha_2)^{s_2}\cdots(x-\alpha_t)^{s_t-1}\neq0.$$

显然

$$d(x)=(f(x),f'(x))=(x-\alpha_1)^{s_1-1}(x-\alpha_2)^{s_2-1}\cdots(x-\alpha_t)^{s_t-1}\neq f(x),$$

从而 $g(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_t)\neq 1$. 所以 $g(x)$ 有与 $f(x)$ 相同的根，且 $g(x)$ 的所有的根都是单根.

10. 证一 1) 因 $f(x)=x^p-x-a$，故由 ch $F=$ 素数 p，$f'(x)=px^{p-1}-1=-1$，从而 $f(x)$，$f'(x)$ 互素. 由第十七章，一，11，1)，$f(x)$ 没有重根.

2) ($\Rightarrow$) 若 $\exists c\in F$，使得 $a=c^p-c$，则 $f(c)=c^p-c-a=0$，即 $f(x)$ 在 F 中有根，从而 $f(x)$ 在 F 上可约，与已知矛盾. 所以 $\forall c\in F, a\neq c^p-c$.

($\Leftarrow$) 假设 $f(x)$ 在 F 上不是不可约，又 $f(x)\neq 0$，$\neq$ 单位，则 $f(x)$ 在 F 上可约. 由第十五章，一，4，注 3)，$f(x)=g(x)h(x)$，其中 $g(x), h(x)\in F[x]$，$0<\deg g(x)<p$，$0<\deg h(x)<p$. 设 E 是 $f(x)$ 在 F 上的一个分裂域，$c(\in E)$ 是 $f(x)$ 的一个根，则 $c+i\cdot 1(i=0,1,2,\cdots,p-1)$ 是 $f(x)$ 的所有根. 事实上，由第十章，三，4，2)，4)，

$$\begin{aligned} f(c+i\cdot 1) &= (c+i\cdot 1)^p-(c+i\cdot 1)-a = c^p+(i\cdot 1)^p-c-i\cdot 1-a \\ &= (c^p-c-a)+(i\cdot 1)^p-i\cdot 1 = 0+i\cdot 1-i\cdot 1 = 0. \end{aligned}$$

若 $c+i\cdot 1=c+j\cdot 1$，其中 $i,j=0,1,2,\cdots,p-1$，$i>j$，则 $(i-j)\cdot 1=0$. 因 $0<i-j\leqslant p-1$，ch $F=p$，故 $(i-j)\cdot 1\neq 0$，发生矛盾. 从而 $c+i\cdot 1\neq c+j\cdot 1(i>j)$. 又 $\deg f(x)=p$，所以 $f(x)$ 共有 p 个不同的根：$c, c+1, c+2\cdot 1, \cdots, c+(p-1)\cdot 1$. 即

$$f(x) = (x-c)[x-(c+1)][x-(c+2\cdot 1)]\cdots[x-(c+(p-1)\cdot 1)] = g(x)h(x).$$

不妨设

$$g(x) = [x-(c+i_1\cdot 1)][x-(c+i_2\cdot 1)]\cdots[x-(c+i_s\cdot 1)],$$

其中 $i_1, i_2, \cdots, i_s\in\{0,1,2,\cdots,p-1\}$，$i_k\neq i_l(k\neq l)$，$0<s<p$. 于是

$$\begin{aligned} g(x) &= x^s-[(c+i_1\cdot 1)+(c+i_2\cdot 1)+\cdots+(c+i_s\cdot 1)]x^{s-1}+\cdots+\prod_{k=1}^{s}(c+i_k\cdot 1) \\ &= x^s-[sc+(i_1+i_2+\cdots+i_s)\cdot 1]x^{s-1}+\cdots+\prod_{k=1}^{s}(c+i_k\cdot 1). \end{aligned}$$

因 $g(x)\in F[x]$，故 $sc+(i_1+i_2+\cdots+i_s)\cdot 1\in F$，又 $(i_1+i_2+\cdots+i_s)\cdot 1\in F$，从而 $sc\in F$. 又因 s 与素数 p 互素，故 $\exists u, v\in\mathbb{Z}$，使得 $su+pv=1$. 于是由 ch $F=p$，有

$$c = c\cdot 1 = c(su+pv) = u(sc)+p(vc) = u(sc)\in F.$$

从而 $\exists c\in F$，使得 $f(c)=c^p-c-a=0$，即 $a=c^p-c$，此与已知条件矛盾. 所以 $f(x)$ 在 F 上不可约.

证二 1) 见证一.

2) ($\Rightarrow$) 见证一.

($\Leftarrow$) 假设 $f(x)$ 在 F 上不是不可约，由证一，$f(x)=g(x)h(x)$，其中 $g(x), h(x)\in F[x]$，$0<\deg g(x)<p$，$0<\deg h(x)<p$. 设 E 是 $f(x)$ 在 F 上的一个分裂域，$c(\in E)$ 是 $f(x)$ 的一个根，则 $f(c)=c^p-c-a=0$，即 $a=c^p-c$. 由已知条件，$c\,\overline{\in}\,F$. 因 c 是 $f(x)$ 的一个根，故 c 是 $g(x)$ 或 $h(x)$ 的一个根，从而 $x-c\mid g(x)$ 或 $x-c\mid h(x)$. 若 $x-c\mid g(x)$. 令 $g(x)=x^s+a_{s-1}x^{s-1}+\cdots+a_0$，则 $g(x)=(x-c)(x^{s-1}+b_{s-2}x^{s-2}+\cdots+b_0)$，$a_0=-cb_0\in F$. 又 $b_0\neq 0$，不然，若 $b_0=0$，则 $a_0=0$，因此 $g(0)=0$，即 $f(0)=0^p-0-a=0$，从而 $a=0$，于是 $a=0^p-0$，$0\in F$，此与已知条件矛盾. 所以 $b_0\neq 0$. 有 $c=-a_0b_0^{-1}\in F$，与 $c\,\overline{\in}\,F$ 矛盾. 若 $x-c\mid h(x)$，同样得出矛盾. 所以 $f(x)$ 在 F 上不可约.

[General Information]
书名=近世代数基础问题探析
作者=齐晓梅，乔凤珠编著
页数=405
SS号=11747628
DX号=
出版日期=2006年9月
出版社=教育科学出版社